Emmanuel Tarantino

Cyber Attack Case Study

On September 7, 2017, one of the major consumer reporting agencies in the United States, Equifax, disclosed that it had been breached. Equifax had found out about the cybersecurity attack on July 29 of the same year, weeks prior their public announcement. In this attack, hackers stole customer names, addresses, birth dates, and even Social Security numbers. The hack reportedly lasted from mid-May to July, during which it was approximated that over 145 million individuals were affected. This number represents roughly half of the United States population. Let us delve deeper into the details of this massive cybersecurity breach, which ranks among one of the largest in the history of the country.

The target of this hack was Equifax, one of the three major consumer reporting agencies in the United States. A consumer reporting agency is an entity that collects and evaluates consumer credit information in order to produce consumer reports. The nature of the business that company such as Equifax conducts requires them to collect and store personally identifiable information, making their databases a treasure trove for any hacker who is able to breach it. As such, a company that wards massive amounts of sensitive information must have advanced anti-hacking measures in place, which begs the question, who sponsored such a sophisticated attack? Unfortunately, even a year and a half later, some questions remain unanswered. Perhaps one of the most unusual aspects of the breach that may shed light on who sponsored the attack is the fact that the stolen data seemingly disappeared. According to an article published by CNBC, experts have two leading theories. The first theory speculates that due to the attention this breach was getting, the hackers who stole the data felt that selling it on the dark web was too risky, and doing so would lead law enforcement to immediately catch them, thus forcing them to just sit on the data. The second theory, which is favored by investigators with an intelligence background, suggest the hackers were working for an unknown foreign nation-state. However, experts who have followed the case closely

believe the truth lies somewhere in the middle. It is possible that the hack was initiated by low-level criminals that found the exploit in Equifax's systems, but did not possess the skills to take advantage of the exploit and move further inside the company's network. As a result, these criminals then sought help via the dark web or other criminal networks, and shared or sold information on the vulnerability to a group of individuals who were probably proxies for the Russian or Chinese government, according to their expert opinion. If this is true, the experts believe the reason why the data has not shown up in the dark web could shed light on the motivation behind the attack. According to them, it is possible that whichever foreign government stole the data is analyzing it using machine learning or artificial intelligence to figure out who is most likely to be, or eventually become, a spy for the United States government. Additionally, credit reporting information contains valuable, compromising data that could be used to leverage individuals and turn them into agents of a foreign government, especially since financial distress is among the top reasons why an individual would commit espionage.

Almost exactly a year after the attack, the United States Government Accountability Office (GAO) produced a report detailing how Equifax was hacked. The attack began in early March 2017, when the hackers were searching the web for any systems that were susceptible to a vulnerability that the United States Computer Emergency Readiness Team had warned about just two days earlier. The vulnerability would allow an attacker to execute commands and relied on an unpatched Apache Struts Web Framework. Approximately two months later, in May, the hackers found that Equifax's online dispute portal software was prime for exploiting this vulnerability. The fact that Equifax may not have been specifically targeted at first lends credibility to the theory that access to the network may have been sold to a foreign nation-state by a group of low-level criminals who hit the jackpot. Then, hackers gained access to the company's online dispute portal, leveraging the system's encryption to blend in their malicious actions with regular activity on the company's network, and launching further attacks without being detected. Eventually, the hackers gained the ability to launch system-level commands on the

dispute portal, issuing queries to other databases, which lead to databases containing personally identifiable information, unencrypted usernames and passwords, and access to several other Equifax databases. According to the report issued by the GAO, Equifax's interim Chief Security Officer confirmed the attackers used this technique to expand their access from the three initial databases associated with the online dispute portal to an additional 48 unrelated databases in the network. Altogether, it was approximated that the attackers had run over 9,000 queries, some of which successfully returned data containing personally identifiable information. The hackers removed this data in small increments, disguising the exchange as regular network traffic, before they were discovered. This lasted for 76 days

Due to the fact that the data seemingly vanished, the ramifications of this massive breach are still hard to measure. There are many financial institutions such as banks, retailers, and lenders, that report credit card activity to Equifax, and as a result, a great number of the 145 million affected consumers may not have been aware the company had their data or that their data had been compromised at the time. In September 2017, Equifax had set up a website to help any individual determine if their information may have been stolen in the breach. Additionally, Equifax announced it would provide free services, such as credit reports and credit monitoring, for one year to all United States consumers regardless of whether or not their information had been compromised in the attack.

Following the 2017 breach, Equifax reportedly took steps to address the vulnerabilities identified in their investigation. According to Equifax officials, once their investigation had concluded and the company identified exactly how the attackers were able to gain unauthorized access to their network and systems, the company took measures to address all the factors that lead to the breach and employ preventive strategies. For instance, one of the steps the company took was to implement a new management process that would identify and patch software vulnerabilities, and confirm these

vulnerabilities have been addressed. Additionally, Equifax implemented a new security tool that would detect incorrect configurations, evaluate any potential signs of a compromise, and automatically signal the IT administrators of vulnerabilities. Equifax officials also stated that a new governance structure would be put into effect in order for the board of directors and senior management to regularly receive risk awareness briefings, requiring the company's Chief Information Security Officer to report directly to the Chief Executive Officer.

The Equifax breach has served as yet another expensive lesson in cybersecurity for the world. As technology rapidly evolves, we find that more of our data is stored in systems and databases, and we trust those systems are safely guarded against hackers with malicious intent. We can only hope that breaches such as this serve as a case study for businesses to take security seriously.

References:

Alfred Ng. “Equifax Data Breach May Affect Nearly Half the US Population.” *CNET*, 7 Sept. 2017, 6:00PM, www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/.

Ng, Alfred. “How the Equifax Hack Happened, and What Still Needs to Be Done.” *CNET*, 7 Sept. 2018, 4:54AM, www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

Ragan, Steve. “Equifax Says Website Vulnerability Exposed 143 Million US Consumers.” *CSO Online*, 7 Sept. 2018, 02:29PM, www.csoonline.com/article/3223229/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html.

Fazzini, Kate. “The Great Equifax Mystery: 17 Months Later, the Stolen Data Has Never Been Found, and Experts Are Starting to Suspect a Spy Scheme.” *CNBC*, 13 Feb. 2019, 3:33PM, www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html.

United States, Congress, Marinos, Nick, and Michael Clements. “Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.” *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, Aug. 2018. www.warren.senate.gov/imo/media/doc/2018.09.06 GAO Equifax report.pdf.