The 2021 Facebook Data Breach

CS 462 - Professor Zehra

Brandon Creech

Old Dominion University

The 2021 Facebook Data Breach

User data is an important asset to protect when serving people. To the public eye, customers rely on companies to protect data, especially when it's the best interest for both of them to prevent hackers from stealing personal information. Customers and companies alike are intertwined when one relies on the other, but complications arise when malicious hackers interfere. This is what arose in 2021, in which Facebook would be found to be a part of a large-scale data breach that affected hundreds of millions of its users with their personal information being exposed. This paper will provide an overview of the incident, what led to it, the details on the technologies used to perpetrate the attack, the consequences it brought, and how this affects today's society.

In 2021, Facebook became the center of controversy as they became involved in a massive data breach that would affect over 530 million users, where they all have reported their data being stolen. This data breach being discovered was bad enough itself; however, what makes it worse is that this data breach was not a sudden incident. This was rather something that built overtime, as the data was begun to have been stolen sometime before August 2019 but was just discovered in 2021. It was a global attack, totaling about 106 countries reporting to have been affected as it targeted general personal information of Facebook users (Bowman, 2021).

This heinous cyber-attack raised questions about how this could happen. How could a cyberattack become this large scale and last this long on a social platform? This can be traced back to 2019, when the attack first started, when the malicious actors found a vulnerability within the platform. Facebook cited in a blogpost that hackers stole the data sometime before September 2019 through using a scraping method on profiles involving synced contacts (Paul, 2021). This "scraping" is a standard method of attack by hackers, in which they essentially harvest, or steal information off of profiles. More than likely, what happened was that they used a harvesting bot program that automates targeting the specific site and steals the data from it (Tester, 2022). The hackers saw the built-in contacts feature for finding friends as an opportunity to apply this method to work. The long-term exploitation of it allowed an accumulation of record data being stolen from hundreds of millions of users. Such vulnerabilities have already validated concerns of Facebook users about the protection of their personal data as there was a previous incident of a data collection violation such as the Facebook-Cambridge scandal. All fingers are now pointed towards Facebook on how they will publicly announce this incident at the very hands of their own mistake.

Not only can we consider Facebook's contact feature to be the technology that was used to perpetrate the attack, but the unaware mind of those involved were also exploited. Humans are perhaps the biggest strength but also can be the biggest weakness when it comes to security. These users on the platform passed along information between each other openly without the concern of security because they believed their profiles would be safe on the platform in the hands of Facebook. However, this is where the trouble began. This created the perfect storm possible for a hacker to take advantage of. We may be able to consider other tools of technology that were used in the attack, although they cannot be confirmed as there is no detailed information about it. An example would be using reconnaissance tools like the Harvester to scope out the platform before making their move, or to potentially look for other vulnerabilities (Sjouwerman, 2022). There is no telling of what exact web scraping program was used, but we can suspect ones like SecretScraper or ParseHub may have been used.

Although the first instinct for a lot of companies in the aftermath of a cyberattack would be to acknowledge it to their users, Facebook decided to take the forbidden route and swept it under the rug. A representative for Facebook announced regarding the data breach that users who were affected would not be notified, as they were not sure exactly on what specific users were affected. This was not a user resolvable issue, and their data still remained as public exposure (Paul, 2021). This brings concern about exactly what kind of trust there is between the users and the companies who look after their data. They are assigned as a pledge to protect user data and ensure it is safe from outsiders. It is one thing for data to be exposed to by a hacker, but for it to happen and to never alert anyone is another concern. Trust is eliminated between the affected users and the company and brings concern to those who are not affected and makes them wonder whether they might be the ones next whose data might be stolen.

This data breach opens doors to other potential cyberattacks that the same hacker or other hackers can take advantage of. Depending on the hacker's motive, they may look to target other parts of Facebook's infrastructure to further cripple the company than it already is, security and financially. Hackers value vulnerabilities within a company's infrastructure, which is why they take the opportunity once they are found and exploit them. A potential aspect of Facebook's security that could be attacked next would be to infiltrate secret information in the company such as financial records or even the microphones on devices of Facebook employees. In Nicole Heron's article, "Media Outlets: An Easy Target in the Eyes of Hackers," she details on how hackers can seize the opportunity to use sensitive information as a strategic advantage. She also detailed on how Galina Timchenko, an exiled Russian journalist serving for an exiled Russian media, had her phone hacked with an application called Pegasus. This caused fears that this could have easily been used to eavesdrop on sensitive information (Heron, 2023). Now, imagine this in the world of Facebook. A hacker could easily do the same thing and eavesdrop in a Facebook meeting via an employee's phone and capture sensitive information regarding financial records or personal information regarding even themselves. It is important to understand that everyone can become a victim of a cyberattack in a company, including the employees as well.

There were immense consequences in the aftermath of this data breach, not just for Facebook but also for today's society. The obvious ones are the loss of trust in Facebook protecting user personal information and their privacy. A company should be able to properly protect this as it is a responsibility that the user entrusts to them and the fact that this was violated now severs that connection. It also provides concerns on the future of technology security as more cyberattacks on as large-scale as the Facebook one could possibly happen in the future. Since technology is constantly evolving, the attacks could forever be increasing in nature. This could mean that this is a catalyst for a higher frequency of data breaches to come because it shows hackers how vulnerable companies can be and how well they can be exploited, which might entice them to attack as well. If we consider how the average cost of a data breach as of 2018 is 8 million U.S. dollars and factor this into how in only the first half of that year more than half of data records being exposed were because of data breaches, it is scary to think what the future holds for society in terms of data security (Team Huntress, 2020).

In conclusion, the 2021 Facebook data breach was a deadly global cyberattack that severely affected both Facebook's reputation and today's society. It was a built-up overtime attack rather than a sudden one as its effects started in 2019, composed of a hacker that exploited the contacts feature on the social media platform, stealing the personal information of users through a scraping method. Facebook's reputation was tarnished when it was discovered that they were originally not planning to notify their users about this data breach. This opened their platform to other potential vulnerabilities that could have been exploited in the aftermath of the attack, such as stealing financial records or eavesdropping on conference meetings between employees using a hacked microphone. Consequences were brought onto today’s society because of this, such as how there are now a severed trust between Facebook and their users over data security and privacy. It also opens doors to larger-scale attacks on both Facebook and other platforms, bringing more fear to users. The attack is a reputation of how deadly cyberattacks have become, and they will only get worse over time as technology evolves. Cyberattacks will only become larger and deadlier in scale, so it is now essential to strengthen infrastructure or else they will become a victim just like Facebook did.

References

Bowman, E. (2021, April 10). *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*. NPR. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Paul, K. (2021, April 8). *Facebook Will Not Notify More Than 530m Users Exposed in 2019 Breach*. The Guardian. https://www.theguardian.com/technology/2021/apr/08/facebook-2019-breach-users

Tester, P. (2022, March 6). *What is Web Scraping? The Ultimate Guide*. https://datadome.co/guides/scraping/what-is-web-scraping-guide/

Heron, N. (2023, November 29). *Media Outlets: An Easy Target in the Eyes of Hackers - salt: Secure communications*. Salt. https://saltcommunications.com/news/media-outlets-an-easy-target-in-the-eyes-of-hackers/

Sjouwerman, S., & 16, S. (2025, March 10). *How Hackers Hack and the Tools They Use - Spiceworks*. Spiceworks Inc. https://www.spiceworks.com/it-security/vulnerability-management/guest-article/how-hackers-hack-and-the-tools-they-use/

Huntress, T. (2020, June 12). *The Impact of Data Breaches on Our Society*. https://www.huntress.com/blog/the-impact-of-data-breaches-on-our-society