**LinkedIn: More than one Apple Short**

James Porter

Department of Computer Science, Southern New Hampshire University

CS 405 Secure Coding

Professor Wasim Alim

September 28, 2022

**Introduction**

In June of 2021, it was first revealed that there was an attack that impacted more than 90% of the user base. The hacker, who has given himself the nickname “God User”, used data scraping techniques to get user data (Hill & Swinhoe, 2021). This attack made headlines, because of the vast number of users that were impacted. Besides this, LinkedIn has been the center of other breaches in the past, which also likely led to more scrutiny from the media.

**Details of the Breach**

From what has been disclosed, there are upwards of 700 million people that were impacted from this breach. Because this is being considered a data scrape, because all the data has been extracted from publicly available information. If this were a data breach, information that is not readily available to the public (e.g., social security number, bank/credit card numbers, etc.) would be taken (What happened on linkedin? 2021). Putting this attack off to the side for a second, there is a growing trend with using LinkedIn as a phishing spot. The long and short of it is that there is trust with LinkedIn and it makes it easier to lure potential victims to other landing pages where they can take their information (Germain, 2022). This may not be the only reason that LinkedIn was targeted, but it is likely one of the many reasons it was used.

**Threats: Immediate and Potential**

There are a lot of threats with this attack and not all of them as immediate as others. I would say that the biggest immediate threat would be that someone buys the information from the user who has it up for sale right now. If someone where to buy this information, they would have access to a lot of information that would allow them to try more tactics to get more information. With the emails from the LinkedIn leak, a malicious user could try and send phishing emails that send users to another landing page to enter their login information only it would send their information to the malicious user. If a user didn’t have proper password etiquette, they could potentially release their login information for countless other accounts that could give the malicious individual even more information (such as a Google account). Another potential threat is that with the email addresses of the users, a malicious individual could brute-force the passwords of a user’s account (LinkedIn data breach - 500M records leaked and being sold 2022).

**Hindsight 20/20**

I think that the biggest change that could have helped reduce the harm in this hack would be if LinkedIn followed the principle of least privilege more stringently. From studying this attack, I have learned that most of this information is readily available to anyone who wanted access to it, and it would only take time to gather than information. Another practice that could have helped would be to have peer accountability. With an attack like this, there had to be a lot of people overlooking a lot of the same issues for it to be successful. One last way that an attack like this could have been mitigated would be if there was a proper security policy in place that kept all the individuals who worked as developers at LinkedIn to the same standard. This would in turn allow individuals who do not follow this policy to be delt with properly.

**Triple A and Defense in Depth**

When it comes down to it, a lot of this attack could have been mitigated with Triple A and defense in depth. This means that we first follow proper authentication practices. If the “God User” account would have been properly identified as a malicious user, they could have prevented this attack from happening. Next, they could have provided proper authorization for the account, or in this case, not authorized the account at all. The first two A’s go hand in hand with the principle of least privilege. The last A is for accounting. This means that there should be some sort of way to track what information goes where. This also means that there is some accountability for the actions that an individual might take (either knowingly, or unknowingly). The last step to ensuring that we provide proper defense in depth. In this example, one of the potential threats is that someone could brute force login information if they had the email address for a user. It might be wise if there were a fail safe to lock the account after a certain number of login attempts.

**Resources**

Cybernews Team. (2022, July 27). LinkedIn data breach - 500M records leaked and being sold. Cybernews. Retrieved September 28, 2022, from https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

Germain, J. M. (2022, May 15). Hackers cast linkedin as most-popular phishing spot. TechNewsWorld. Retrieved September 28, 2022, from https://www.technewsworld.com/story/hackers-cast-linkedin-as-most-popular-phishing-spot-176643.html

Hill, M., &amp; Swinhoe, D. (2021, July 16). The 15 biggest data breaches of the 21st Century. CSO Online. Retrieved September 28, 2022, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

What happened on linkedin? JD Supra. (2021, July 29). Retrieved September 28, 2022, from https://www.jdsupra.com/legalnews/what-happened-on-linkedin-3826345/