LinkedIn data breach

During 2021, LinkedIn was the target of 2 data breach incidents resulting in more than 90% of its users base being compromised as data associated with LinkedIn accounts was posted on a dark web forum. The biggest incident was reported in June 2021 where around 700 million accounts were affected. After an initial analysis of the information found on the dark web, LinkedIn announced that the site did not include any sensible information like financial data or login credentials and argued that the fact that data related with LinkedIn accounts ended in the site was due to hackers taking advantage of public facing data available to everyone on their end and the later efforts to get the remaining information from other sources.

An investigation made by other sources found that the data publicized in the dark web forum did included set of sensible personal information including:

- Full names
- Phone numbers
- Physical addresses
- Email addresses
- Geolocation records

The bad actor behind this attack is believed to have used data scraping techniques exploiting LinkedIn's API. Weirdly enough, it is believed the hacker manage to use the same technique for both of the attacks, the first taking place in April 2021, suggesting that LinkedIn haven't address the issue properly.

It is unclear what concrete actions LinkedIn has taken to address the problem since the official posture of the company is that the incident wasn't a data breach and that no user private data was exposed. In their official press communicate the company emphasizes that data scraping is a violation of LinkedIn terms of service and if anyone tries to use user data for purposes outside of the user data agreement the company will hold them accountable.