Source : www.thehindu.com Date : 2018-10-07

IS FACEBOOK DATA BREACH SERIOUS?

Relevant for: Security Related Issues | Topic: Basics of Cyber Security and related matters

What happened?

On September 16, Facebook noticed an unusual spike in the number of times the platform’s ‘View As’ feature was being used. The feature allows users to see how their Facebook page will appear to another user. On September 25, Facebook announced that it had identified this as a malicious activity in which the access tokens of 50 million users were appropriated by unknown hackers, and certain personal details possibly accessed.

What is an access token?

An access token is a digital key that allows users to stay logged into Facebook on a device or browser without having to sign in repeatedly using their password. It extends its reach to other apps or services that users sign into using their Facebook account. If hackers have the access tokens, they do not require passwords to get into Facebook accounts or apps like Instagram that utilise the Facebook login.

What did hackers do?

The ‘View As’ feature was introduced by Facebook as a privacy control feature, allowing users to check the information they were sharing with others. But this proved to be an Achilles’ heel because of some bugs that were introduced in the software in July 2017. According to Techcrunch, while using the ‘View As' feature, Facebook’s video uploader tool also appeared on the page at times, generating an access token that was not the user's but of the person the user was looking up. For example, if Hacker A selected User B for ‘View As,’ and the video uploader appeared on the page, it generated an access token for User B which was then available to Hacker A.

What was Facebook’s response?

Facebook had to force the affected 50 million users, and an additional 40 million users who had used the ‘View As’ feature since last July to log in again so that their access tokens changed. Facebook has since said it has resolved the bugs that caused what is said to be the largest breach in the history of the platform. Facebook is said to be working with the FBI on the issue. It also informed the Irish Data Protection Commission, since the European Union’s strict new data protection law states that it has to be informed within 72 hours if anyone in the European Economic Area is affected. The Commission has started a probe, and Facebook faces a fine that could go over a billion dollars.

Why is it significant?

This breach again puts the spotlight on the vulnerabilities of Facebook, the digital behemoth that claims over two billion users and along with Google controls more than half of the global digital advertisement revenue. It was caught on the wrong foot earlier this year when the Cambridge Analytica scandal broke, revealing that data of up to 87 million users were harvested and used for political campaigning. There are ongoing investigations into that scandal, and the new breach is not helping Facebook redeem itself. Aside from the direct impact of private data being accessed, massive data sets allow for psychological profiling a la Cambridge Analytica. This could lead to targeted political advertising and manipulation, especially at a time when crucial mid-term elections are due in the United States and in India. It also undermines the faith in the ‘single sign-in.’ The Facebook sign-in has been utilised by a whole set of services, from gaming apps to news apps, as a way to log in to their sites or apps based on the idea that large digital entities like Facebook and Google provide better security. This trust now stands shaken. While Facebook has reportedly refreshed the access tokens of all affected parties, the extent to which the hackers had access to connected third-party apps remains unclear.

P.J. George

END