Source : www.thehindu.com Date : 2021-04-16

EXPLAINED

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

Facebook logo is reflected in a drop on a syringe needle in this illustration photo taken March 16, 2021. | Photo Credit: Reuters

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

Facebook has suffered yet another data breach, only this time, private information from 533 million accounts have been leaked online. Even the company's founder and CEO Mark Zuckerberg's private credentials are part of the larger leaked data set from 2019.

Also read: Ireland launches inquiry into Facebook after reports of data leak

Here is a look at the nature of this data leak, ones similar to it, and their impact on netizens:

Private information of users was primarily obtained by exploiting Facebook's contact importer feature that allows users to find friends on social media using their phone's contact list.

Malicious actors exploited a weakness in the feature to gain access to user ID, address, phone number, email address, names of workplaces, date of birth, date of account creation, and other personal identifiable information. They then leaked this data in the dark web. Information on users' finance and password were not divulged.

All 533,000,000 Facebook records were just leaked for free.

This means that if you have a Facebook account, it is extremely likely the phone number used for the account was leaked.

I have yet to see Facebook acknowledging this absolute negligence of your data. https://t.co/ysGCPZm5U3 pic.twitter.com/nM0Fu4GDY8

Facebook claims hackers obtained user data through data scraping — a process used by people to import data from a website onto a local file that is saved in a computer. The social networking giant also noted in a blog post that "the specific issue that allowed them [hackers] to scrape this data in 2019 no longer exists."

"A lot of companies like Facebook, Google and others provide their APIs to developers for several reasons. Hacker groups essentially use them to scrape data from these sites," said Rajshekhar Rajaharia, a Rajasthan-based entrepreneur and cybersecurity researcher, in an email to *The Hindu*.

"They can procure the name and email of a particular user from one website through their API, A second website's API might provide them with their phone number and address, a third might open the doors to more sensitive information on the same user. Hackers are essentially combining these details and creating a complete data set which is then being sold online."

The latest instance stands out for the sheer number of accounts compromised. According to a report published by Business Insider, personal information of over half a billion Facebook users in 106 countries was leaked online. This includes over 32 million records on users in the U.S.,

11.5 million in the U.K., and 6 million in India.

Earlier, data of 500 million LinkedIn users were being sold online by an unknown hacker who had dumped two million users' data as sample. Separately, online stock trading company Upstox's data was stolen due to compromised Amazon Web Service (AWS) keys.

This hack includes users' Aadhaar and PAN credentials, passport soft copy, bank account numbers, and photos of signatures, Rajaharia noted.

"In the case of LinkedIn, it was asserted that data was scraped, in other words, someone violated the terms of service to cull out data from the public profile, combined with data from other sites," Raj Samani, Chief Scientist at cybersecurity firm McAfee told *The Hindu*.

The information leaked is in many ways similar to Facebook's leak, but it contains other professional information that might add another layer of sensitivity.

The stolen information can be used to send spam emails, make calls, mount phishing campaigns and target advertising. It can be used to plot and execute various nefarious online fraud schemes. Hackers can impersonate users and transfer cash on their behalf, without their knowledge.

The database of private information is available on dark web for anyone to sift through. CTO of cyber intelligence firm Hudson Rock in early January confirmed that this data was now being sold on various groups on the cloud-based messaging app Telegram. Recently the data set seems to be popping up on various hacker forums all across the internet.

Internet users seeking to know whether their data has been leaked or compromised, can visit HaveiBeenPawned.com. All they have to do is to key in their email id and check.

The FB breach has certainly generated some interest, currently doing 40k-45k requests per min on @haveibeenpwned (up about 6x on normal baseline traffic) pic.twitter.com/Rpa8itUwsh

Also, people can use Google Passwords to analyse login patterns to know whether their account was breached.

Please enter a valid email address.

Since the backlash from its users began in January, WhatsApp has been trying hard to get them back on its platform, by using several methods including reaching out to users via the "status" feature

END