50 million user accounts hacked in Facebook data breach

Kevin Reed
5 October 2018

Facebook reported on September 28 that hackers had exploited a technical flaw in the social media platform and obtained the user information of about 50 million accounts. In this largest ever breach since the company was founded 14 years ago, the hackers found a security hole in the "View As" feature—that allows users to see what their profile looks like from other Facebook accounts—to gain access to login details.

Among the hacked accounts were those of Facebook founder and CEO Mark Zuckerberg and Facebook COO Sheryl Sandberg. In a Security Update blog post on Facebook's Newsroom page, VP of Product Development Guy Rosen wrote that the hackers had used the "View As" feature to "steal Facebook access tokens which they could then use to take over people's accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don't need to re-enter their password every time they use the app."

Rosen further explained that the vulnerability had been fixed, that law enforcement had been notified of the breach and that a thorough security review was being conducted to determine if the compromised accounts had been accessed or misused. The access tokens of both the affected 50 million accounts as well as another 40 million accounts that have been subject to the "View As" look-up in the last year have been reset, Rosen said.

One of the more troubling aspects of the hack is that access to Facebook account details can also enable access to many other user accounts. For example, there are hundreds of apps—among the most popular are Spotify and Instagram—that allow people to use Facebook credentials as a third-party login to their other accounts.

As in the report last spring of the harvesting of personal Facebook data by Cambridge Analytica, the Facebook "View As" hack is being seized upon as further evidence of Russian meddling and to demand government intervention and control of social media. Some news outlets immediately began raising the likelihood of "rogue state" involvement in the breach without presenting any evidence backing it up.

Virginia Democratic Senator Mark Warner released a statement on the same day that Facebook made the announcement that said, "This is another sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users." Additionally, the Irish Data Protection Commission opened a formal investigation into the data breach under the terms of the European Union's General Data Protection Regulation (GDPR) that could result in a fine of up to $1.63 billion.

During a conference call, Facebook executives reported that company engineers noticed a problem on September 16 when an unusual "spike in traffic" appeared on their systems. It was not known initially if this spike was evidence of malicious activity. According to the executives, it took another nine days before the engineers uncovered the massive security breach.

Security experts familiar with the complex technical issues involved in the Facebook hack have said that it may be impossible to trace the source of the attack or "connect the dots" in order to identify the hackers.

Over the past year and a half, Facebook has increasingly cooperated with the US government and state intelligence agencies in promoting the unsubstantiated claims of anti-Russian meddling during the 2016 elections and the need to promote "trusted sources" in opposition to "fake news." More recently, Facebook worked with the Digital Forensic Lab of the

Atlantic Council to shut down pages, posts and accounts connected with a purported, but still unproven, Iranian influence campaign.

These efforts are part of a broader drive to censor left-wing speech across all social media platforms, gather intelligence on political activists and create a framework for disabling accounts and publishing activity deemed “divisive” or “inauthentic.” The technology monopolies and the state fear that the social media platforms will be used increasingly as tools for coordinating and organizing the growing social and political struggle of the working class and young people. The recent data breach—regardless of who is responsible for it—plays directly into these strategic aims of the ruling elite and strengthens the instruments of censorship and state repression.