0-The New York Times-Facebook

Facebook Security Breach Exposes Accounts of 50 Million Users

Send any friend a story

As a subscriber, you have 10 gift articles to give each month. Anyone can read what you share.

Give this article

287

Read in app

One of the challenges for Facebook’s chief executive Mark Zuckerberg is convincing users that the company handles their data responsibly.Credit… Josh Edelson/Agence France-Presse — Getty Images

By Mike Isaac and Sheera Frenkel

Sept. 28, 2018

SAN FRANCISCO — Facebook, already facing scrutiny over how it handles the private information of its users, *[Anger]* said on Friday that an attack on its computer network had exposed the personal information of nearly 50 million users.

The breach, which was discovered this week, was the largest in the company’s 14-year history. The attackers exploited a feature in Facebook’s code to gain access to user accounts and potentially take control of them.

The news could not have come at a worse time for Facebook. It has been buffeted over the last year by scandal, from revelations that a British analytics firm got access to the private information of up to 87 million users

to worries that disinformation on Facebook has affected elections and even led to deaths in several countries.

Senior executives have testified several times this year in congressional hearings where some lawmakers suggested that the government will need to step in if the social network is unable to get tighter control of its service. On Friday, regulators and lawmakers quickly seized on the breach to renew calls for more oversight.

“This is another sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users,” Senator Mark Warner *[Disappointment]*, a Democrat from Virginia and one of Facebook’s most vocal critics in Congress , said in a statement. “A full investigation should be swiftly conducted and made public so that we can understand more about what happened.”

In the conference call on Friday, Guy Rosen, a vice president of product management at Facebook, declined to say whether the attack could have been coordinated by hackers supported by a nation-state. *[Deny]*

Three software flaws in Facebook’s systems allowed hackers to break into user accounts, including those of the top executives Mark Zuckerberg and Sheryl Sandberg, according to two people familiar with the investigation but not allowed to discuss it publicly. Once in, the attackers could have gained access to apps like Spotify, Instagram and hundreds of others that give users a way to log into their systems through Facebook.

[Read more about what you can do to secure your Facebook account.]

The software bugs were particularly awkward for a company that takes pride in its engineering *[Worry]*: The first two were introduced by an online tool meant to improve the privacy of users. The third was introduced in July 2017 by a tool meant to easily upload birthday videos.

Facebook said it had fixed the vulnerabilities and notified law enforcement officials. *[Rebuild]* Company officials do not know the identity or the origin of the attackers, nor have they fully assessed the scope of the attack or if

particular users were targeted. The investigation is still in its beginning stages.

“We’re taking it really seriously,” Mr. Zuckerberg, the chief executive, said in a conference call with reporters. “I’m glad we found this, but it definitely is an issue that this happened in the first place.”

Critics say the attack is the latest sign that Facebook has yet to come to terms with its problems. *[Disappointment]*

“Breaches don’t just violate our privacy. They create enormous risks for our economy and national security,” *[Disappointment]* Rohit Chopra, a commissioner of the Federal Trade Commission, said in a statement. “The cost of inaction is growing, and we need answers.”

Facebook has been roundly criticized for being slow to acknowledge a vast disinformation campaign run by Russian operatives on its platform and other social media outlets before the 2016 presidential election.

Ms. Sandberg, Facebook’s chief operating officer, testified in a Senate hearing that month about what the company was trying to do to prevent the same thing from happening in midterm elections in November.

In April, Mr. Zuckerberg testified about revelations that Cambridge Analytica, the British analytics firm that worked with the Trump presidential campaign, siphoned personal information of millions of Facebook users.

Outside the United States, the impact of disinformation appearing on Facebook and the popular messaging service it owns, WhatsApp, has been severe. In countries such as Myanmar and India, false rumors spread on social media are believed to have led to widespread killing.

Facebook said the attackers had exploited two bugs in the site’s “View As” feature, which allows users to check on what information other people can see about them. The feature was built to give users move control over their privacy.

The company said those flaws were compounded by a bug in Facebook's video-uploading program for birthday celebrations, a software feature that was introduced in July 2017. The flaw allowed the attackers to steal so-called access tokens — digital keys that allow access to an account.

It is not clear when the attack happened, but it appears to have occurred after the video-uploading program was introduced, Facebook said. The company forced more than 90 million users to log out early Friday, a common safety measure taken when accounts have been compromised.

The hackers also tried to harvest people's private information, including name, sex and hometown , from Facebook's systems, Mr. Rosen said. The company could not determine the extent of the attackers' access to third-party accounts, he said.

Facebook has been reshuffling its security teams since Alex Stamos, its chief security officer, left in August for a teaching position at Stanford University. Instead of acting as a stand-alone group, security team members now work more closely with product teams across the company. The move, the company said, is an effort to embed security across every step of Facebook product development. *[Rebuild]*

Part of that effort has been to gird Facebook against attacks on its network in preparation for the midterm elections. Facebook has spent months setting up new systems to pre-empt such attacks, and has already dealt with a number of incidents believed to be connected to elections in Mexico, Brazil and other countries.

Still, the recently discovered breach was a reminder that it is exceptionally difficult to entirely secure a system that has more than 2.2 billion users all over the world and that connects with thousands of third-party services.

"This has really shown us that because today's digital environment is so complex, a compromise on a single platform — especially one as popular and widely reaching as Facebook — can have consequences that are much more far-reaching than what we can tell in early days of the investigation," *[Worry]* said April Doss, chairwoman of cybersecurity at the law firm Saul Ewing.

As the news of Facebook's data breach spread quickly across Twitter, Google searches and other online sites, there was one place where it remained difficult to find some detailed reports: Facebook. *[Diminish, Disappointment]*

Users who posted breaking stories about the breach from The Guardian, The Associated Press and other outlets were prompted with a notice that their posts had been taken down *[Deny]*. So many people were posting the stories, they looked like suspicious activity to the systems that Facebook uses to block abuse of its network.

"We removed this post because it looked like spam to us," the notice said .