What comes next in Facebook's major data breach

September 29 2018, by Matt O'brien And Mae Anderson

In this May 1, 2018, file photo, Facebook CEO Mark Zuckerberg makes the keynote speech at F8, Facebook's developer conference in San Jose, Calif. Facebook says it recently discovered a security breach affecting nearly 50 million user accounts. In a blog post, Friday, Sept. 28, the company says hackers exploited its "View As" feature, which lets people see what their profiles look like to someone else. Facebook says it has taken steps to fix the security problem and alerted law enforcement. (AP Photo/Marcio Jose Sanchez, File)

For users, Facebook's revelation of a data breach that gave attackers

access to 50 million accounts raises an important question: What happens next?

For the owners of the affected accounts, and of another 40 million that Facebook considered at risk, the first order of business may be a simple one: sign back into the app. Facebook logged everyone out of all 90 million accounts in order to reset digital keys the hackers had stolen—keys normally used to keep users logged in, but which could also give outsiders full control of the compromised accounts.

Next up is the waiting game, as Facebook continues its investigation and users scan for notifications that their accounts were targeted by the hackers.

What Facebook knows so far is that hackers got access to the 50 million accounts by exploiting three distinct bugs in Facebook's code that allowed them to steal those digital keys, technically known as "access tokens." The company says it has fixed the bugs.

Users don't need to change their Facebook passwords, it said, although security experts say it couldn't hurt to do so.

Facebook, however, doesn't know who was behind the attacks or where they're based. In a call with reporters on Friday, CEO Mark Zuckerberg—whose own account was compromised—said that attackers would have had the ability to view private messages or post on someone's account, but there's no sign that they did.

"We do not yet know if any of the accounts were actually misused," Zuckerberg said.

The hack is the latest setback for Facebook during a tumultuous year of security problems and privacy issues . So far, though, none of these

issues have significantly shaken the confidence of the company's 2 billion global users.

This latest hack involved bugs in Facebook's "View As" feature, which lets people see how their profiles appear to others. The attackers used that vulnerability to steal access tokens from the accounts of people whose profiles came up in searches using the "View As" feature. The attack then moved along from one user's Facebook friend to another. Possession of those tokens would allow attackers to control those accounts.

One of the bugs was more than a year old and affected how the "View As" feature interacted with Facebook's video uploading feature for posting "happy birthday" messages, said Guy Rosen, Facebook's vice president of product management. But it wasn't until mid-September that Facebook noticed an uptick in unusual activity, and not until this week that it learned of the attack, Rosen said.

"We haven't yet been able to determine if there was specific targeting" of particular accounts, Rosen said in a call with reporters. "It does seem broad. And we don't yet know who was behind these attacks and where they might be based."

Neither passwords nor credit card data was stolen, Rosen said. He said the company has alerted the FBI and regulators in the United States and Europe.

Jake Williams, a security expert at Rendition Infosec, said he is concerned that the hack could have affected third party applications.

Williams noted that the company's "Facebook Login" feature lets users log into other apps and websites with their Facebook credentials. "These access tokens that were stolen show when a user is logged into Facebook

and that may be enough to access a user's account on a third party site," he said.

Facebook confirmed late Friday that third party apps, including its own Instagram app, could have been affected.

"The vulnerability was on Facebook, but these access tokens enabled someone to use the account as if they were the account-holder themselves," Rosen said.

News broke early this year that a data analytics firm once employed by the Trump campaign, Cambridge Analytica, had improperly gained access to personal data from millions of user profiles. Then a congressional investigation found that agents from Russia and other countries have been posting fake political ads since at least 2016. In April, Zuckerberg appeared at a congressional hearing focused on Facebook's privacy practices.

The Facebook bug is reminiscent of a much larger attack on Yahoo in which attackers compromised 3 billion accounts—enough for half of the world's entire population. In the case of Yahoo, information stolen included names, email addresses, phone numbers, birthdates and security questions and answers. It was among a series of Yahoo hacks over several years.

U.S. prosecutors later blamed Russian agents for using the information they stole from Yahoo to spy on Russian journalists, U.S. and Russian government officials and employees of financial services and other private businesses.

In Facebook's case, it may be too early to know how sophisticated the attackers were and if they were connected to a nation state, said Thomas Rid, a professor at the Johns Hopkins University. Rid said it could also

be spammers or criminals.

"Nothing we've seen here is so sophisticated that it requires a state actor," Rid said. "Fifty million random Facebook accounts are not interesting for any intelligence agency."