5-CNN-Facebook

Facebook just had its worst hack ever — and it could get worse *[Worry]*

By Donie O’Sullivan, CNN Business

Updated 9:22 AM EDT, Thu October 4, 2018

New York

CNN

—

On Sunday, September 16, engineers at Facebook detected some unusual activity on the social media platform’s networks. It was an attack, the biggest security breach in Facebook’s history. And it would take the company 11 more days to stop it.

Now, almost a week since the public was first told of the attack, we still barely know anything about what happened. *[Disappointment]*

We don’t know who the hackers were, or what they were looking for. We don’t know whether they were targeting particular people in certain countries. We don’t know how long they had access to users’ information. And we don’t know what, if anything, they took. *[Disappointment]*

What we do know is that for at least 50 million users, the hackers could have seen everything. They could have logged in as if they were those users, and then accessed years of those users’ activity history on the platform — including their private messages.

Things could get very ugly. *[Worry]* The hackers could be trolls who decide to post a database of millions of people’s private messages online for everyone to read. They could be Russian intelligence, gathering information from politicians' personal accounts and then sitting on it until just the right moment to wreak havoc on the midterm or 2020 elections. They could be blackmailers, combing through the messages of high-value targets like politicians, government officials, and wealthy individuals.

Or maybe none of that is true. We might learn that the attackers didn't access all the information that was exposed, or that they weren't as sophisticated as feared, that they were just playing around, or that they never quite realized how potentially earth-shaking their accomplishment was. They might never do anything with the information they stole — or they may never have stolen anything at all.

The attackers figured out how to exploit three separate vulnerabilities in Facebook's code. Facebook said last week it didn't know when the hackers had figured it all out, but that the vulnerabilities had existed since July 2017.

What the attackers did before Facebook (FB) found and fixed the vulnerabilities may determine the social media company's future.

Soon, Facebook will have to give the public, lawmakers and regulators, not just in the US but all over the world, answers to some very big questions.

Was September 16, the day the engineers noticed something was amiss, the beginning of the attack? Were the hackers siphoning off data for the 11 days took Facebook to fix the problem? Or, even worse, were the attackers in the system long before Facebook ever detected something was wrong?

The worst scenario for Facebook and its users is that the attackers had unfettered access to 50 million accounts for an extended period of time and knew exactly what they were doing.

If the hackers want to undermine Facebook or cause it lasting damage — or simply create chaos — they could at any time post the private information of millions of people openly online.

Hackers did something like that in 2015 to Ashley Madison, a dating site for people cheating on their partners, posting a searchable database of email addresses registered to accounts on the website. The public disclosure of that kind of private information can have tragic and permanent consequences; some people caught up in the Ashley Madison hack committed suicide.

When the Cambridge Analytica scandal broke earlier this year, it prompted a global outcry and Facebook's stock tumbled 18%. That story did have the allure of a pink-haired whistleblower and Cambridge's ties to the Trump campaign. But this breach, which has gotten far less attention, could impact many more people than Cambridge did.

Facebook relies on trust. People trust that their pictures will be seen only by those in their networks, that their private messages will be read only by the people to whom they were sent. Facebook may look like a juggernaut now, but social networks have fallen before, and if this attack destroys that trust, the company could quickly find itself in dire straits. *[Disappointment]*

Figuring out who the attackers were and what they did and didn't do is now paramount for the company.

One of the most important objectives after discovering an attack is "stopping the bleeding," Shawn Henry, an FBI veteran who is the president of the cybersecurity firm CrowdStrike Services, told CNN Business. CrowdStrike was hired by the Democratic National Committee after it was hacked during the run-up to the 2016 election.

"You want to establish how deeply infiltrated the environment is, what has the adversary compromised, are they still there? How long have they been there?" he said, speaking not about the Facebook breach specifically, but about his experience running investigations into cyber intrusions.

We may never know who attacked Facebook. We may never know whether they stole personal information. Or we may learn the answers to both — in public and, for tens of millions of people, far too late. *[Disappointment]*