From: [redacted]
Sent: 12 October 2018 18:55
To: [redacted]
Cc: European Data Protection Board;[redacted]
Subject: Re: Facebook security announcement

Dear Chairwoman Jelinek,

At 18:30 CET today, we published an update about our investigation into the attack we announced on September 28. As we explained in our initial announcement, attackers exploited a vulnerability that allowed them to steal Facebook access tokens. 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.

Today, we provided an update on the impact of the attack we've found that exploited this vulnerability. Please note that we have not ruled out the possibility of smaller-scale attacks, which we're continuing to investigate.

We now know that fewer people were impacted than we originally thought. Of the 50 million people whose access tokens we believed might have been exposed at the time, about 30 million actually had their tokens taken.

We also explain how the attack happened:

First, the attackers already controlled a set of accounts, which were connected to Facebook friends. They used an automated technique to move from account to account so they could steal the access tokens of those friends, and for friends of those friends, and so on, totaling about 400,000 people globally. In the process, however, this technique automatically loaded those accounts' Facebook profiles, mirroring what these 400,000 people would have seen when looking at their own profiles. That includes posts on their timelines, their lists of friends, Groups they are members of, and the names of recent Messenger conversations. Message content was not available to attackers, with one exception. If a person in this group was a Page admin whose Page had received a message from someone on Facebook, the content of that message was available to the attackers.

The attackers used a portion of these 400,000 people's lists of friends to steal access tokens for about 30 million people. For 15 million people, attackers accessed two types of information – name and contact details (phone number, email, or both depending on what people had on their profiles). For 14 million people, attackers accessed the same two types of information, as well as other details people may have had on their profiles. This included username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches. For 1 million people, attackers did not access any information.

People will be able to check whether they were affected by visiting our Help Center. In the coming days, we will send customized messages to the 30 million people affected to explain what information the attackers might have accessed, as well as steps they can take to help protect themselves, including from suspicious emails, text messages, or calls.

This attack did not include Messenger, Messenger Kids, Instagram, Oculus, Workplace, Pages, third-

party apps, or advertising or developer accounts, though we are still investigating how it may have impacted Groups.

We hope this update is helpful. Please note that we have shared this information with our lead Supervisory Authority, the Irish DPC. The DPC will be in contact with relevant concerned supervisory authorities as appropriate.

Kind regards,

[redacted]
Privacy and Public Policy, EMEA

[redacted]

From: [redacted]
Date: Friday, September 28, 2018 at 6:05 PM
To: [redacted]
Cc: "edpb@edpb.europa.eu" , Erin Egan , [redacted]
Subject: Re: Facebook security announcement

With apologies, I am re-sending the email with the correct address for the EDPB Secretariat.

From: [redacted]
Date: Friday, September 28, 2018 at 5:58 PM
To: [redacted]
Cc: "edpb@edpb.europa.edu" , [redacted]
Subject: Facebook security announcement

With copy to the EDPB Secretariat

Dear Chairwoman Jelinek,

I wanted to make sure that you saw our announcement that, on the afternoon of Tuesday, September 25, our engineering team discovered an attack on our systems by an external actor. We are continuing to investigate this attack. We provide more information in this Newsroom post: https://newsroom.fb.com/news/2018/09/security-update/. We will update this post when we have more information, or if the facts change.

We have reported this information to our lead Supervisory Authority, the Irish DPC, in accordance with Article 33 of the General Data Protection Regulation (GDPR). The DPC is evaluating the information we have shared with them, and have informed us they will be in contact with relevant concerned supervisory authorities as appropriate.

Please let us know if you have any questions.

Regards,

Privacy and Public Policy, EMEA
Facebook