FACEBOOK, INC.

Moderator: Caryn Marooney
September 28, 2018 10:00 a.m. PT

Mark Zuckerberg: Thank you, everyone, for joining us today.

I want to update you on an important security issue we've identified. We patched the issue last night and are taking precautionary measures for those that might have been affected. We're still in the early phase of investigating this, but in the interest of transparency we want to share everything we know now.

On Tuesday afternoon, our engineering team found an attack affecting up to 50 million accounts on Facebook. The attackers exploited a vulnerability in the code of the View As feature which is a privacy feature that lets people see what their Facebook profile would look like to another person. The vulnerability allowed the attackers to steal Facebook access tokens -- which are the equivalent of a digital key -- which the attackers could have used to take over or access people's accounts.

The investigation is still very early. We do not yet know if any of the accounts are actually misused. So far, our initial investigation has not shown that these tokens were used to access any private messages or posts or to post anything to these accounts. But this, of course, may change as we learn more. The attackers did try to query our APIs to access profile information fields -- like name, gender, hometown, et cetera -- but we do not yet know if any private information was accessed that way. We're continuing to look into this and we will update when we learn more.

Now, this is a serious issue and we've already taken a number of steps to address this.

First, we patched the security vulnerability to prevent this attacker -- or any other attacker -- from being able to steal additional access tokens. And we invalidated the access tokens for the accounts of the up to 50 million people who were affected, causing those people to be logged out. These people will now have to log back in to access their accounts again and we will also notify

these people in a message on top of their News Feed about what happened when they log back in.

Second, as a precautionary measure -- even though we believe we've now fixed the vulnerability -- we're temporarily taking down the whole View As feature that had the vulnerability in it until we can fully investigate it and make sure that there are no other security issues or vulnerabilities there.

Third, as an additional precautionary measure, we're also logging out everyone who used the View As feature since the vulnerability was introduced last year. This will require another 40 million people -- or more -- to log back into their accounts.

Fourth, we're in touch with law enforcement to help identify the attackers. While we don't yet know who's behind the attack, we're working to understand more details about what happened and who is responsible, and we will update you with more details when we have them.

The reality here is we face constant attacks form people who want to take over accounts or steal information. I'm glad we identified this one, fixed the vulnerability and secured the accounts that may be at risk. But we need to do more to prevent this from happening in the first place. And it's part of our ongoing focus to be more proactive about taking reasonability for the safety of our community. We're going to keep investing very heavily in security going forward.

That's the summary of what we know now. And now I'm going to hand over to Guy Rosen to answer any questions that you may have.

Operator: Your first question comes from Sarah Frier from Bloomberg. Please go ahead.

Sarah Frier: Hi.

I just want to get a little bit more clarity on what you -- what you mean by effecting almost 50 million accounts -- and you said that there was no evidence of data misused -- but what do you mean by affecting?

Guy Rosen: What we mean is that for almost 50 million accounts, we have seen that these access tokens were taken. What we're seeing is 50 million of those. And additionally we are also taking the step of resetting not only those access tokens, but also access tokens for an additional 40 million accounts that have been subject to a View As look up as a precautionary step -- all of these (just as) steps to help protect the security of people's accounts.

Operator: Your next question comes from the line of Paresh Dave from Reuters.

Paresh Dave: Hey there.

Was wondering if you can be more specific on the type of law enforcement that you notified? Was it the National Security Council or any national security officials?

Guy Rosen: We're working with the FBI and with law enforcement; we will update when we learn more from these interactions.

Operator: Your next question comes from the line of Mike Isaac from the New York Times. Please go ahead.

Mike Isaac: Hey, guys. Thanks for taking my question.

This is kind of for Mark, just for -- just because of an earlier quote. But, Mark, I think -- I'm just thinking back to your testimony in congress and one of the main points you made was if Facebook's here to serve its users and if you can't be responsible with user data then you don't deserve to serve users. And I guess I'm just wondering if you still think you all are able to do that because it just -- it seems like a pretty -- another pretty big breach of user trust?

Thanks so much.

Mark Zuckerberg: Yes. Thanks, Mike.

This is a really serious security issue. And we're taking it really seriously. We have a major security effort at the company that hardens all of our surfaces,

and investigates issues like this. In this case I'm glad that we found this and that we were able to fix the vulnerability and secure the accounts. But it definitely is an issue that this happened in the first place.

This underscores the attacks that our community and our service face, and the need to keep on investing heavily in security, and being more proactive about protecting our community. And we're certainly committed to doing that.

Operator: Your next question comes from the line of Josh Constine from TechCrunch. Please go ahead.

Josh Constine: Hi.

Were any EU users affected such that this would constitute a GDPR breach?

And earlier today, a hacker said that they were planning to hack Mark Zuckerberg's profile live over Livestream. Does this breach have anything to do with that hacker or was he able to plan this attack using anything based off of this attack?

Guy Rosen: On your first question, we've notified the Irish Data Protection Commission in accordance to the obligations we have under GDPR.

On the second part of your question, we're not aware that this -- that that person was related to this attack at all.

Operator: Your next question comes from the line of Issie Lapowsky from WIRED, please go ahead.

Issie Lapowsky: Hi. Thank you for taking my question.

You said when you discovered that this breach happened, but do you have any idea when the breach took place?

And separately, can you walk through the process of how you determine whether these tokens were in fact used to access personal information?

Guy Rosen: Yes, thanks for the question.

Let me -- let me walk through the timeline of how this played out. The vulnerability itself, which was a result of three distinct bugs -- which I can walk over later -- was introduced in July, 2017, when we created the new -- a new video upload functionality on the service. In -- on September 16th, we discovered some unusual (activity -- this is) something like a spike in users -- and we launched an investigation.

On the afternoon of this week's Tuesday, September 25th, we uncovered this attack and we found this vulnerability. And then on Wednesday, we notified law enforcement yesterday, Thursday afternoon, Thursday evening, we fixed the vulnerability, and we began resetting the access tokens of people to protect the security of their accounts. This is also causing people to be logged out of Facebook and they will have to log back in.

Operator: Your next question comes from the line of Donie O'Sullivan from CNN. Please go ahead.

Donie O'Sullivan: Hey, guys.

Do we have any idea of (where the) users that are impacted by this are based -- is it mostly American users?

Guy Rosen: Thanks for the question.

Given this investigation's still early, we haven't yet been able to determine if there's specific targeting. It does seem broad and we don't yet know who is behind these attacks or where there's base -- or where they might be based.

Operator: Your next question comes from the line of Sean Gallagher from Ars Technica. Please go ahead.

Sean Gallagher: Thanks for taking the call.

As far as the bug goes, you said it was introduced as art of the video upload feature. Was it -- was there any other dependencies that this was associated with?

And you already addressed the fact that you don't know who was (targeted yet) but do you have any idea of how the attack was launched in terms of a specific source or if it was -- if you -- if it was going after a particular profile of users who had done videos?

Guy Rosen: Thanks.

Let me walk through the vulnerability and how it actually manifested.

Taking a step back to provide some context, our site like almost any other site uses a mechanism called access tokens. An access token is not a -- not your password; it's kind of like a digital key that keeps you logged in to Facebook so that every time you open the app, you don't need to reenter your password. Now, parts of our site use a mechanism called single sign-on -- SSO -- that creates a new access token. And the way this works is, for example, let's say I'm logged in to the Facebook mobile app and it wants to open another part of Facebook inside a browser.

What it will do is it will use that single sign-on functionality to generate an access token for that browser. That means you don't have to log in again into that browser window. Now, the vulnerability itself was the result of these three distinct bugs and the interaction between them, and it was introduced, as I said, in July 2017 through a video uploader.

Let me walk through those three bugs.

The first bug was that, when using the View As function to look at your profile as another person would, the video uploader shouldn't have actually shown up at all. But in a very specific case, on certain types of posts that are encouraging people to post happy birthday greetings, it did show up.

The second bug was that this video uploader incorrectly used the single sign-on functionally, and it generated an access token that had the permissions of the Facebook mobile app. And that's not the way the single sign-on functionality is intended to be used.

The third bug was that, when the video uploader showed up as part of View As -- which it wouldn't do were it not for that first bug -- and it generated an access token which is -- again, wouldn't do, except for that second bug -- it generated the access token, not for you as the viewer, but for the user that you are looking up.

It's the combination of those three bugs that became a vulnerability. Now, this was discovered by attackers. Those attackers then, in order to run this attack, needed not just to find this vulnerability, but they needed to get an access token and then to pivot on that access token to other accounts and then look up other users in order to get further access tokens.

This is the vulnerability that, yesterday, on Thursday, we fixed that, and we're resetting all of those access tokens to protect security of people's accounts so that those access tokens that may have been taken are not usable anymore. This is what is also causing people to be logged out of Facebook to protect their accounts.

Operator: Your next question comes from the line of David McCabe from Axios. Please go ahead.

David McCabe: Thanks for taking the question.

I'm wondering what impact do you expect this to have on your year-long efforts to win back the trust of regulators and lawmakers around the world?

And as a more specific follow-up to that, have you notified anyone else besides the Irish Data Protection Authority and the FBI?

Guy Rosen: Look, this is a -- this is clearly a breach of trust, and we take this very seriously. We're working with lawmakers and with regulators to let them know about what happened.

Operator: Your next question comes from the line of Dustin Volz from the Wall Street Journal. Please go ahead.

Dustin Volz: Hi. Thank you.

Yes, I just want to get back the hack itself. Can you describe how sophisticated you think these actors were or what kind of resources they would've had to employ to discover these three discrete bugs, as you mentioned? Any expectation or suspicion that this was a nation state?

Guy Rosen: I think our -- the investigation is early, and it's hard to determine exactly who was behind this, and we may never know. This is a complex interaction of multiple bugs that happened together. It did -- it did need a certain level in order for the attacker to run this attack in a way that not only gets access tokens, but then pivots on those access tokens and continues to further -- get further access tokens using this mechanism.

We're going to continue investigating, and as we find more, we will share what we know.

Operator: Your next question comes from the line of Laura Hautala from CNET. Please go ahead.

Laura Hautala, your line is open.

Laura Hautala: I'm sorry; I was on mute. Thank you for taking the question.

I'm wondering if you can tell me more about once user -- or once attackers were pivoting through these accounts -- first of all, I'm wondering if this had to be done just one by one, step by step, or if there was any way to scale this attack up?

And second of all, I'm wondering if what they were able to access then also had to be manually collected, or was there any level of automation or speed that could be introduced to take advantage of this on a higher level?

Guy Rosen: Thanks for the question.

We did see this attack being used at a fairly large scale, and that's how we discovered this and we are -- and we started investigating and ultimately found the vulnerability and the attack that was happening. In terms of the data, look, given it's early we don't yet know exactly how accounts were

misused so far. We haven't seen that the access tokens were used to access private messages or posts or post anything to the accounts, but it is still early and that may change.

What we know is the attackers did try to use the APIs to access profile information -- like name or gender or hometown -- but it's important to say the attackers could use the account as if they are the account holder. And our investigation is still early. We're going to determine how these accounts were misused and what information was taken.

Operator: Your next question comes from the line of Kate Fazzini from CNBC. Please go ahead.

Kate Fazzini: Hi.

I'm interested in knowing how long you think it'll be until you know whether any of those compromised accounts were used?

Guy Rosen: Our investigation's still early; we will update as we find more.

Operator: Your next question comes from the line of Casey Newton from The Verge. Please go ahead.

Casey Newton: Hey. Thanks.

Guy, follow-up there, if the attackers could use the account as a legitimate account holder, does Facebook have any way of accurately determining what is legitimate usage versus illegitimate usage for the purposes of determining whether they accessed private posts or not?

Guy Rosen: This is part of our investigation. We're -- what we're doing is understanding the different access tokens and how they were used and how they were issued. This is not a simple investigation, and this is why we're going to continue investigating in order to find and understand how accounts may have been misused.

Operator: Your next question comes from the line of Tamsin McMahon from The Globe and Mail. Please go ahead.

Tamsin McMahon: Hi. Thanks very much for organizing this call.

I was just wondering -- so if this was related to a vulnerability based on changes that were made back in July of 2017, I'm curious why it took so long to identify this, given it's been more than a year since this update was made?

And also I wanted to clarify whether -- how you first identified it? If I understand correctly, it was through a spike in new users being registered, or was it just in overall user activity?

Thank you.

Guy Rosen: Thanks for the question.

Security vulnerabilities are by definition -- they're obscure and they're very hard to find. And when we build products we bake security in from the start, we use secure coding libraries -- that means that there's less likelihood to be these bugs -- we do code reviews, we run static analysis tools that can catch some issues. But regrettably it didn't catch this complex interaction of bugs that led to this vulnerability.

On the second part of your question, the original investigation started when we saw a pattern of usage -- increased user access to the site, and then when we dug in to understand that, we found that this was in fact driven by an attack that was exploiting this vulnerability.

Operator: Your next question comes from the line of Carlos Fernández from Expansión. Please go ahead.

Carlos Fernández: Hi, everyone.

I want to ask to complement what Mark said in the previous call with what happened with Cambridge Analytica, (that time they say that you want to be around to help) the security teams inside of Facebook. I remember it was around 20,000 -- 20,000 people (all around the world). I wanted to know if these (new vulnerabilities -- these new -- if these new -- if these new) hacking has changed anything, the amount of people that they're going to be hiring,

(security)? (And) I want to understand when you say that you are increasing the amount of security, what does it mean for the company?

Guy Rosen: We're committed to investing in safety and security. This is incredibly important, including hiring, and we're going this year from 10,000 to 20,000 people working on safety and security. Working with people, including engineers, security analysts, content reviewers -- this is a very important part of the work that we do and we have a big responsibility to take these issues seriously.

Operator: Your next question comes from the line of Kurt Wagner from Recode. Please go ahead.

Kurt Wagner: Hey, thanks.

This question's for Mark. I think this is the third security-related incident that I can remember even just since June. I'm wondering why should users continue to trust Facebook with their personal information?

Mark Zuckerberg: This is -- this is a -- is a serious issue and we're -- and we're very focused on addressing it, which is why we patched the vulnerability and taken additional precautionary measures, including taking down the feature where the vulnerability was in it until we can fully investigate it and make sure that that's secure. And we're also logging out an additional number of people that we currently don't have any evidence that their accounts were compromised in any way, but (we're) -- just as an extra precautionary measure.

This is, as I've said in a number of our -- number of the things I've written in and spoken about, including election security -- security is a bit of -- it's an arms race. And we're continuing to improve our defenses and I think that this also underscores that there are just constant attacks from people who are trying to take over accounts or steal information from people in our community.

And I think that the teams that we have at Facebook are very focused on this and there are a lot of talented people who are working on this and I think

doing good work. But this is going to be an ongoing effort we're going to need to keep on focusing on this over time.

Operator: Your next question comes from the line of Martin Untersinger from Le Monde. Please go ahead.

Martin Untersinger: Hi. Thanks for taking my question.

Is there anything Facebook users should do right now to secure their account like changing their passwords?

Guy Rosen: Thanks for the question.

No, passwords were not taken. We are resetting these access tokens for users who were affected and so they will be logged out of Facebook and they will have to log back in again. That protects the security of their accounts.

Operator: Your next question comes from the line of the Davey Alba from Buzzfeed News. Please go ahead.

Davey Alba: Hi. Thanks so much for doing this.

You mentioned that the attackers could have accessed name, gender and hometown information of profiles. Do you have any guesses what they could -- these attacker could be using that information for? Could it be of interest, for instance, an advertiser?

And additionally, can you expand on the 40 million other accounts that could have been subjected to the View As (lookup) -- what specifically kind of data could be taken from those accounts?

Guy Rosen: Yes. Thanks for the question.

The -- to explain, the -- what we have seen so far is that the attackers used the standard profile retrieval API and -- which basically shows what you have on your profile, your -- the fields that are there. And that includes information like name, or gender or hometown. We don't yet know exactly (if) they're

using those or if it's just one part of perhaps a multiple set of steps that they may be taking or plan to take in the future.

The -- but again, we don't know exactly how -- which and how -- what information we will find has been used. What we've seen so far is that access tokens were not used to access things like private messages, or posts, or to post anything to these accounts and we'll update as we learn more.

On your -- your second question, so to clarify -- to add one more thing there, the -- what we also can confirm is that no credit card information has been taken. We do not display credit card information, even to account holders. And so, that is also safe.

On the second part of your question, we've also taken the -- sorry, so 50 million accounts were directly affected by this attack and we know the vulnerability was used against them. And we're resetting the access tokens for those accounts, so people will be logged out. The other 40 million people are people who have been subject to a View As lookup. That means someone else used View As to lookup their profile. To be safe, as we are still investigating this activity, we are -- we took that precautionary step of resetting their access tokens.

Operator: Our last question at this time comes from the line of Steven Levy from WIRED. Please, go ahead.

Steven Levy: Hi. Thanks for setting this up and taking the call.

Recent -- in the last year, you've reorganized the security somewhat. When your chief security officer was in the process of leaving, I know that you did that. Has that -- did that -- looking back at this -- and I know it's early for this -- would that have had any effect on how quickly you found this vulnerability? Or going forward, are you going to take another look at how the reorganization went?

Guy Rosen: Yes, so look, people's privacy and security is very important. And we're taking this very, very seriously and investing heavily in it. And that's why, as you said, we have embedded our security folks -- engineers, analysts,

investigators -- into our product and engineering teams so that we can better address these emerging threats.

If anything, we think that means we were able to find and address this faster. And in general with these things, the harder -- the harder you look, the more you will find. And so we are looking, and we are finding and we are responding fast. And it's very important for us to share what we found as part of that as well.

Caryn Marooney: Thank you, all, for joining us today. For more information, we have our Newsroom which has the Newsroom post so please follow-up there.

Thank you.

Operator: This concludes the Facebook Press Call. Thank you for joining. You may now disconnect your lines.

END