FACEBOOK, INC.

Moderator: Tom Reynolds
September 28, 2018
2:00 p.m. PT

Operator: This is Conference # 2888486

Operator: Hello and welcome to today's Facebook Press Call.

There will be prepared remarks and a Q&A to follow. To ask a question after the prepared remarks conclude, please press "star," "one."

Now, I'd like to turn the call over to Tom Reynolds, who will kick this off.

Tom Reynolds: Thanks, operator. And hi, everybody. Thanks again for joining us and apologies for the slight delay. This is Tom Reynolds from the Facebook Communications team.

Since our call this morning, we've had some technical questions which we felt would be easier to answer in person with some of our experts here on the call. With me is Guy Rosen, Vice President of Product Management who oversees safety and security here at Facebook and Nathaniel Gleicher, Facebook's Head of Cybersecurity Policy.

We're going to do the same drill as earlier -- a few brief remarks followed by your questions. This is also on the record and with no embargo. And when you ask your question, please state your name and your publication, please.

With that, I'll turn it to Guy to get us started.

Guy Rosen: Thanks, Tom.

Here's some additional technical details that we wanted to share.

Firstly, we've been getting a lot of questions about the -- how View As works -- and it is complicated. This is a privacy feature that lets people see what their own profile looks like to someone else. For example, if you have friend, View As enables you to view your account through that person's eyes and that lets you check exactly what they could see.

Once the attackers had an access token for one account, let's say (Alice's), they could then use View As to see what another account, let's say, (Bob's), could see about (Alice's) account. Due to the vulnerability, this enabled them to get an access toke for (Bob's) account as well, and so on and so on.

And second, we've had a lot of questions about the three bugs I referenced this morning, so I'll run through those again.

Our site, like many others, uses a mechanism called access tokens. This is not your password; it is kind of a digital key that keeps you logged into Facebook so that you don't need to reenter your password every time you use the app. And parts of our site use a mechanism called single sign-on -- or SSO -- to create new access tokens. The example is if I'm logged into the Facebook mobile app and it wants to open another part of Facebook inside a browser window, it can use SSO to generate an access token for that browser, which means you don't have to enter your password again.

The vulnerability that we -- that we fixed was the result of three distinct bugs, and it was introduced in July of 2017 when we created a certain new video uploader. Here's the three bugs.

The first bug was that when using the View As product, the video uploader actually shouldn't have shown up at all, but in a very specific case around posts that encouraged people to wish happy birthdays, it did show up.

Now, the second bug was that this video uploader incorrectly used SSO -- that single sign-on product -- to generate an access token that had the permissions of the Facebook mobile app. That's not how SSO was intended to be used on our platform.

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

It's the combination of these three bugs that created a vulnerability. This vulnerability was discovered by hackers, and the way they exploited it is not just finding this vulnerability and using it to get an access token, but then every time they have an access token pivoting from that to other accounts, other friends of that user to get further access tokens.

With that, that's it for me. Let's take questions.

Operator: We will now open the line for questions. Please limit yourself to one question per person. To ask a question, press "star" followed by the number "one."

Your first question comes from the line of Will Oremus of Slate. Please go ahead.

Will Oremus: Hi. Will Oremus from Slate Magazine.

I wanted to know what are some of the potential concerns once somebody has that access token for your account?

And one specific question I had as a follow-up is could they have used it to log in with Facebook to other accounts on the web that used a Facebook login?

Thanks.

Guy Rosen: The vulnerability was on Facebook, but these access tokens enabled someone to use the account as if they were account -- the account holder themselves. This does mean they could have accessed other third-party apps that were using Facebook login. Now that we have reset all of those access tokens as part of protecting the security of people's accounts, developers who used Facebook login will be able to detect that those access tokens have been reset,

identify those users, and as a user, you will simply have to login again into those third-party apps.

Operator: Your next question comes from the line of Mike Cappetta of NBC News. Please go ahead.

Mike Cappetta: Thanks for taking my question.

I was curious, is there any connection is to WhatsApp or Instagram with this breach?

Guy Rosen: The -- like I said, the vulnerability was on Facebook itself. And we've yet to determine, given the investigation is really early, whether there were -- what were the exact nature of misuse and whether there was any access to Instagram accounts, for example. Instagram, the behavior with Instagram would be similar to what I described earlier around a third-party app and if you have a Facebook account that has been affected which is linked to an Instagram account, what you have to do today is to unlink and relink that account to Instagram.

There was no impact on any WhatsApp users at all.

Operator: Your next question comes from the line of Matt O'Brien of the Associated Press. Please go ahead.

Matt O'Brien: Hi.

You just said that these -- it could have been used to access other third-party apps. Do you have evidence that it was?

Nathaniel Gleicher: We are early in the investigation. Our first focus on this was to understand the full scope of users that could have been impacted and make sure that they were secure. And so that's what we're focused on at this point.

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

Issie Lapowsky: Hi. Thanks.

Sorry, when you say you have to unlink and relink the Instagram accounts or any other Facebook family accounts that you have, does that mean you didn't automatically reset those accounts for users that were affected? They have to do it manually?

Guy Rosen: To be clear, once we have reset the access tokens on Facebook, those accounts are protected. However, if you would like for example to crosspost from Instagram to Facebook, in order for that to work you will need to unlink and relink that Instagram account to Facebook.

Operator: Your next question comes from line of Hannah Kuchler of Financial Times. Please go ahead.

Hannah Kuchler: Hi there.

How will you be investigating what data could've been lost through third-party apps since you have so many?

Nathaniel Gleicher: Our first step here is to make sure that we know who was impacted and that we've taken steps as quickly as we can to ensure that they're secure. We're very early in the investigation. Our next priorities are understanding the full scope of impact to look into what activity could've behind this. And as we develop that investigation and as that proceeds, we'll be continuing to report out.

Operator: Your next question comes from the line of Glenn Chapman of AFP. Please go ahead.

Glenn Chapman: Hi. Thanks for stepping up again to deal with these technical questions.

The -- I'm just -- can you just you give me a like a use case -- a better (like, color) use case scenario -- somebody goes on Facebook and wishes somebody a happy birthday with the automated system and this kicks in? I'm just trying to get for regular users who might not be that tech savvy, what do they have to set these dominos going?

And then just if you could say it was first -- you first noticed this spike in activity or the thing that caught your attention was September 16th? That's (being reported); if you can confirm that or not, that would help.

Guy Rosen: Thanks for the question.

To be clear, the way the work that the attack works is that the attacker -- not a specific user -- accessed the View As feature on their account and would then be able to get the access tokens through the sequence of bugs that turned into the vulnerability to someone who is their friend.

They could then, in order to use this attack, take that access token, and then not only use it, but pivot from that access token, log-in as the next user, and then try to get access to their friends. There's nothing a specific user would do in order to be compromised; this is (some -- an attack) that starts from the attacker's side.

On your second question, yes, on September 16th, we started investigating a certain spike in traffic, and that led to, on Tuesday, us finding this attack. And then we acted very swiftly. And by yesterday -- Thursday evening -- we fixed the vulnerability that we had identified and we began logging users out in order to reset their access token, which is what we need to do in order to protect the security of people's accounts.

Operator: Your next question comes from the line of Heather Kelly of CNN. Please go ahead.

Heather Kelly of CNN, please go ahead.

Your next question comes from the line of Robert McMillan of Wall Street Journal. Please go ahead.

Robert McMillan: Oh, hi there.

If I understand this correctly then, as a Facebook user, if one of my friends was compromised through this series of bugs, then my -- the data that I had that I thought was private would've been shared with the hackers. Could you

tell me how many people are in that situation where their data may've been available to the hackers just because they friends of these 50 million -- or 90 million accounts?

Guy Rosen: No. The accounts whose access tokens were taken are (that count) -- the 50 million accounts whose access tokens were taken -- those accounts we have gone ahead and we have logged them out of Facebook. And we are notifying those users in order to protect the security of those accounts.

Operator: Your next question comes from the line of Hillary Vaughn of Fox Business. Please go ahead.

Hillary Vaughn: Hi. Thank you so much for taking my question.

Are you guys optimistic that you will be able to find out if these attackers actually accessed people's private direct messages? And if so, will you notify those users, individually, about what information was probed into?

Nathaniel Gleicher: That's a great question.

As we've said -- so the investigation is still early. Part of -- because we wanted to move so quickly in this space, we really wanted to focus on making sure we knew who had been affected so we could make sure they were secure. The investigation's proceeding now so we can understand access or what types of activities were taken. As with any investigation in this space, it can be challenging to understand the full scope of activity. As we run this and as we understand more, we will absolutely be ensuring that we can share as much as we can.

Operator: Your next question comes from the line of Molly McHugh of The Ringer. Please go ahead.

Molly McHugh: Hi. Thanks, guys.

One question I have is that, it looks like there are a lot of people reporting they were automatically logged out this morning, early, early, early this morning, (later the) morning -- in the morning -- and that they were not giving

any reasons why. They didn't see that notification ever. I'm wondering if there was a reason it's happened or if you -- if it's just rolling out slower, so if we could get some clarification on that, that would be great.

Guy Rosen: We began logging users out last night Pacific Time in order to start protecting the security of people's accounts. We are rolling out those notifications on the top of people's feed and they will receive those.

Operator: Your next question comes from the line of David Lee of BBC News. Please go ahead.

David Lee: Hi there. Thanks for taking the question.

I just wanted to know if your investigation will include looking at how these bugs were allowed to exist in the system, whether there'll be any action taken and accountability at Facebook for what happened?

Nathaniel Gleicher: One of the things that's really clear is that there are sophisticated adversaries that are determined to try to find a way into any system like this. We are continually focused on finding vulnerabilities like that and when we find them, moving as quickly as we can to ensure that they're fixed and ensure that the users are secure. That's what we did in this case; we moved from confirmation of an exploit to actually fixing the vulnerability and securing the accounts just in a couple of days. And our goal going forward is to continue to do that same thing.

Operator: Your next question comes from the line of Joe Menn of Reuters. Please go ahead.

Joe Menn: Hi, guys.

What did you learn from scraping the accounts that the attackers used to launch the penetration and did you see any exfiltration that was associated back to those indicators?

Nathaniel Gleicher: That's a good question, Joe.

We're just starting, as we've said, to work through the full scope of what we've seen here. What we've seen so far, this appears to be a pretty broadly focused range of accounts that were affected. And our next step now is to dig into a lot of those questions that you're asking.

As we understand more about this, we'll be following-up.

Operator: Your next question comes from the line of Alex Heath of Cheddar. Please go ahead.

Alex Heath: Hey. Thanks for taking my question. Alex Heath with Cheddar.

You guys have said several times that you're early in the investigation; you don't know everything. I am curious, can you give us a more detailed sense of the timeline of why it took you, I guess, four days to disclose this to the public and a couple days to actually reset people's accounts? What was the process? Did you have to notify law enforcement first? Can you -- can you walk us through those days this week?

Nathaniel Gleicher: Yes. We went from confirming that there was an active attack on the evening of Tuesday to fixing the vulnerability and beginning to secure user accounts by Thursday. It was actually a very quick turnaround. During that time, we did notify law enforcement. We identified and patched that vulnerability. And we started and began a process, not just to identify all the users that were implicated, but to ensure that they were protected.

When you're talking about the scope and scale of this type of investigation, we drove this very quickly. And one of the things we found, actually, is that as we brought our security teams and our product teams closer together, (it essentially) allowed us to run an investigation like this as fast as we think we possibly could have.

Operator: Your next question comes from the line of Alina Selyukh of NPR. Please go ahead.

Alina Selyukh: Hi.

On the numbers 50 million you're saying were affected -- almost 50 million -- those additional 40 million that you are logging off, what exactly is the concern about those accounts?

Guy Rosen: To clarify, 50 million are the accounts are the accounts that we've confirmed have been affected by this attack and the additional 40 million are users who have interacted with that View As product where the vulnerability existed. We're taking a -- as a -- out of an abundance of caution -- the step of resetting their access tokens as well.

The goal of all of this in logging all of these people out of Facebook is to protect the security of their accounts.

Operator: Your next question comes from the line of Margi Murphy of Telegraph. Please go ahead.

Margi Murphi: Hi, there.

I just wanted to be clear -- you said that on the 16th of September you noticed (soaring) traffic and that's what opened -- led you to investigate what was going on. Was it over a 24-hour time period that these 50 million access tokens were stolen?

And (separate to that), are you aware of -- there's a number of YouTube videos which advise people what to do with -- or how to steal access tokens and how to hack into accounts, and are you working with Google to remove them?

Thanks.

Guy Rosen: On the 16th we detected that spike in traffic, which launched our initial investigation. It wasn't clear at that point there was any malicious activity happening and it was on Tuesday of this week that we found there was an attack. And as Nathaniel said, we moved very quickly to address it and by Thursday we were logging people out of the site in order to protect the security of their accounts.

There -- on your -- the second part of your question, there are certain videos out there that may be describing different elements not referring to this kind of vulnerability. We're certainly looking into all of these and want to make sure that people's accounts are protected on Facebook.

Operator: Your next question comes from the line of Jessica Guynn of USA Today. Please go ahead.

Jessica Guynn: Hi. Thanks very much for giving us some extra time.

I'm wondering is it possible that more than the 50 million accounts that you've identified were breached in the attack, or do you expect that number to grow?

And also I was wondering if you could tell us -- I know that you're notifying 90 million people, but of the 50 million whose users -- whose accounts were breached, will they be notified that they were in fact affected that way?

Thanks.

Guy Rosen: Thanks for the question.

Again, the 50 million were the number of accounts that were directly affected by this account. And exactly in order to be cautious and make sure that we are -- that we're acting with caution and protecting the security of anyone who may have been affected -- that is why we're taking action on those additional 40 million in order to protect the security of their accounts as well.

Operator: Your next question comes from the line of Matthew Braga of CBS News. Please go ahead. CBC News, my apologies.

Matthew Braga: Yes, that's OK.

Just to be clear, so if someone had used one of these tokens to access an account, would that have showed up in the Facebook settings that show where all of the devices that are currently accessing an account are logged in? And if not, why not?

Guy Rosen: I'm sorry, Matthew, do you mind repeating that?

Matthew Braga: Yes, sure, I'm just wondering -- Facebook has that page in the settings that shows the IP address, the location of all the different devices that are currently logged into your Facebook account. And I'm wondering if someone was using one of these access tokens to access someone's account, would it have showed up in that settings page that shows all the places that your Facebook account is being accessed from?

Guy Rosen: Hey, thanks for the question.

It depends on how that access token was being used. If they went through what is a technical step of creating a -- what we call a full web session -- from that access token, it would indeed have shown up. There are some other cases where it may not have shown up if it was used, similar to how a developer might access a certain account only in order to perform certain very limited parts of the functionality.

It's worth pointing out that the -- at the bottom of that list, there is a button that says log out of all sessions -- that does clear and reset all of the access tokens on the account similarly to the action that we proactively took over the past 24 hours and protects the security of those accounts.

Operator: Your next question comes from the line of Jonathan Vanian of Fortune. Please go ahead.

Jonathan Vanian: Hey. Thanks, guys, for doing this again.

This is kind of a semantics question, but I know this is a bit different than the Cambridge Analytica that was sort of a British -- or, sorry -- a breach of trust issue and this seems to be a hack. Can you just tell us in regard to the scale, like how does this compare to previous hacks on Facebook? Is this the biggest hack that the company has experienced, given the amount of accounts that were compromised?

Guy Rosen: Look, this is something that we're taking very, very seriously, and we moved very fast from the moment we learned that there was an attack and we are

going to continue to investigate this in order to learn more about what happened and what kind of data was accessed.

Operator: Your next question comes from the line of Brian Feldman of New York Magazine. Please go ahead.

Brian Feldman: Hey, thanks for doing this.

Just to go back to the issue of how you guys are notifying users, I was wondering why you guys are only placing a notification on the top of the feed and not e-mailing users or doing else like that. Why should I have to log back in to a compromised account in order to find out?

Nathaniel Gleicher: This is the most efficient way to ensure that users can see the information right at the top of their feed when they login. And this is actually the best way to do it at scale. We're talking about 90 million user accounts here. We wanted to make sure that we could both execute the logout and make it so that when they log back in easiest for them to fully understand what has happened.

Operator: Your next question comes from the line of Kelsey Sutton of Ad Week. Please go ahead.

Kelsey Sutton: Hi. Thank you for taking my question.

I have a couple numbers that I just want to get clarity on. You said that the first bug was because of a patch to a video uploading thing -- the birthday video of July 2017, and then September 16th is where you -- September 16th, 2018 is where you saw the spike in traffic and then September 25th was when you determined that there had been a breach. Were the 60 million users compromised between July 2017 and today? Was it only September 16th through the 25th, was it only the 25th? Can you provide any sort of information as to how long these accounts were compromised for?

Guy Rosen: Thanks for the question.

We are going back and we are looking for all of the users who may have been affected by this, and that is how we reached that number, the 50 million

accounts that were affected directly by an attack and 40 million accounts who had interacted the View As part of our product and we're logging all of those people out in order to protect the security of their accounts.

Operator: Your next question comes from the line of Catalin Cimpanu of ZDNet. Please go ahead.

Catalin Cimpanu: Good afternoon. Thank you for taking my question.

Are the compromised accounts located in a specific area of the globe?

Guy Rosen: Given the investigation is still fairly early, we haven't yet been able to determine if there's a specific pattern. The early indication make it seem like it is very broad and there is no specific country or area targeted, but it is still early days. And as we learn more, we will update with what we learn.

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

Russell Brandom: Yes, thanks for doing this.

I have two quick ones. One is, you're referring to the 50 million accounts as sort of the work of, essentially, a single attacker. How confident are you that this vulnerability was not exploited by other attackers, potentially, I guess?

And then, also, is your understanding that this is going to have implications under the GDPR as a data breach from a policy perspective?

Guy Rosen: All right, so on the first question. The 50 million were the accounts that we've confirmed have been implicated and attacked. We are still early in the investigation, and we are not able to tell, is there one attacker, multiple attackers. We are working to learn more about who and what entities might've been behind those .

On your second question, we've notified the Irish Data Protection Commission in accordance with our obligations under GDPR.

Operator: Your next question comes from the line of Michelle Quinn of Voice of America. Please go ahead.

Michelle Quinn: Hi. Thank you so much.

Somebody asked my question, but I did want to just double check that (The Journal) reported that the breach was the biggest that Facebook's ever faced?

Thank you.

Nathaniel Gleicher: We're early in this investigation, and we're working through the full impact. What we've seen is, as I've said, 50 million users that were directly impacted and an additional 40 million that were exposed to the vulnerability. And so, our focus has been, let's make sure that we get those 90 million people secured. And now we're moving to sort of better understand the full scope and other implications.

Tom Reynolds: Thanks. Operator, we're going to have time for two more questions please.

Operator: Certainly. Your next question comes from the line of Michael Kan of PC Magazine. Please go ahead.

Michael Kan: Hi. This is Michael with PC Magazine.

I was wondering if Facebook had a -- well, Facebook said that you noticed it on September 16 when you were -- when the attacker was scraping the accounts. Has Facebook had a chance to look deeper and to see if the attacker was scraping accounts before the September 16TH date, if this had been going on for a while, just on a smaller scale?

Guy Rosen: Our investigation is still very early, so we don't yet know exactly the scope of the misuse and how and if accounts were actually misused. We're aware of a fairly large attack which is, as you said, what drove a spike in traffic and drew our attention to this. We are looking throughout the time period where this vulnerability existed in order to learn more and we will share more as our investigation unfolds.

Operator: Your final question comes from the Brian Krebs of Krebs on Security. Please go ahead.

Brian Kerbs: Hi. Thanks for doing this. This is Brian Krebs.

I'm looking at a Facebook post from an individual who seems to been credited by Facebook for reporting security vulnerabilities in the past. And he put a post on Facebook, on September 17, claiming to have discovered and reported this vulnerability to Facebook then.

Can you talk about whether Facebook received any kind of official notification from a researcher about this or any kind of bug bounty request at around the same time it detected a spike in traffic?

Thank you.

Nathaniel Gleicher: Sounds like that may be unrelated to what we're talking about here. I mean from what we -- this was the result of our analysis, starting first with this unusual activity that keyed us in to look more deeply, and then the confirmation as of this Tuesday evening, that there was an attack (under process).

Tom Reynolds: All right. With that, we're going to have to wrap up. Thank you, everyone, for joining us.

If you have follow-up questions, you can reach us at press@fb.com.

Thank you again and thank you, operator.

Operator: This concludes the Facebook press call. Thank you for joining. You may now disconnect your line.

END