

[← Previous article](#)[Next article →](#)

## Twitter Hack Update: What We Know (and What We Don't)



Author:

Tara Seals

July 17, 2020 / 1:36 pm

Share this article:



With limited confirmed information, a raft of theories and circumstantial evidence has come to light as to who was behind the attack and how they

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

Joe Biden, Bill Gates, Elon Musk, Apple, Uber and others, after it became clear that hackers had

been able to compromise them. The tip-off? Suddenly these high-profile accounts were all tweeting out identical links to a cryptocurrency scam.

But what exactly happened? As Threatpost **reported on Wednesday**, Twitter's internal investigation is ongoing, but the social-media giant did say that hackers had somehow compromised the company's internal systems and secured employee privileges. Beyond that, a raft of sources are offering bits and pieces of the puzzle – some verified, some not.

On Saturday, **Twitter posted a 900-word summary of the attack** outlining what it knows. It stated that the company was hit with a social engineering "scheme" targeting a small number of employees. Those targets were manipulated to perform "certain actions" and divulge confidential information.

**Threatpost Today!** Daily headlines delivered to your inbox

Subscribe now

"The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. As of now, we know that they accessed tools only available to our internal support teams to target 130 Twitter accounts," Twitter wrote. "For 45 of those accounts, the attackers were able to initiate a password reset, login to the account, and send Tweets."

Attackers accessed the Twitter account feature "**Your Twitter Data**" for eight accounts. However, for the "vast majority" of compromised accounts the unknown adversaries were unable to access private account information, according to Twitter.

In a summary of what was accessed Twitter wrote:

- *Attackers were not able to view previous account passwords, as those are not stored in plain text or available through the tools used in the attack.*
- *Attackers were able to view personal information including email addresses and phone numbers, which are displayed to some users of our internal support tools.*
- *In cases where an account was taken over by the attacker, they may have been able to view additional information. Our forensic investigation of these activities is still ongoing.*

It added over the weekend it was working to unlock and restore those affected accounts. The

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

Thursday night, the tech behemoth offered some additional details as part of the above support feed.

"Based on what we know right now, we believe approximately 130 accounts were targeted by the attackers in some way as part of the incident," it tweeted. "For a small subset of these accounts, the attackers were able to gain control of the accounts and then send Tweets from those accounts."

It added, "We're working with impacted account owners and will continue to do so over the next several days. We are continuing to assess whether non-public data related to these accounts was compromised, and will provide updates if we determine that occurred."

And, "For all accounts, downloading Your Twitter Data is still disabled while we continue this investigation."


The FBI is taking the lead in the investigation, [according to Reuters](#), after several lawmakers expressed dismay over the larger ramifications of the incident.

That's it for solid factual evidence. But there's plenty of connect-the-dots circumstantial information to flesh out what may have happened.

### ***What we might know:***

Prior to the account takeovers, hackers known to be active in the SIM-swapping community tweeted out screenshots of Twitter's internal dashboards. These are the same tools that could have been used to carry out Wednesday's attack, allowing the ability to hijack Twitter accounts, associate new email addresses with them and avoid two-factor authentication (2FA) protections.

[SIM-swapping](#) or SIM-jacking is a method of bypassing SMS-based 2FA to crack high-value accounts. A typical attack involves calling a target's mobile carrier – easily discovered with an online search – and asking to port the line to a different SIM card/device, using previously phished information to "verify" their identity. It's a successful gambit, given that many carriers [don't ask in-depth security questions](#) that fully verify that the caller is in fact the legitimate cell phone user; also, many SIM-swappers resort to bribery or extortion to achieve their goals, or they [cultivate malicious employees](#).

 We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

Krebs also said that an unnamed “mobile industry security source” told him that PlugWalkJoe in real life is a 21-year-old from Liverpool. This individual is allegedly named Joseph James Connor, and he is reportedly currently residing in Spain because he was there at university when the pandemic hit and has been stuck there ever since.

Meanwhile, a somewhat different narrative emerges in an investigation by Vice/Motherboard. That outlet said that screenshots of Twitter’s internal tools appeared on underground forums ahead of the attacks (and confirmed the screenshot tweets from compromised OG accounts that Krebs mentioned). It also claimed to have sources inside the hacker group responsible for the campaign, who said they merely bribed a Twitter employee and were off to the races.

“We used a rep that literally done all the work for us,” one of the sources told Motherboard. The outlet backed up the claim with information from a “Twitter spokesperson” who confirmed that this was a malicious inside job, and said that the company is still investigating whether the employee hijacked the accounts themselves or gave hackers access to the tool.

Twitter however denied the rogue employee theory, instead insisting that employee(s) merely fell for a social-engineering scam. it **tweeted out** after the Motherboard piece went public that ““We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools.”

## ***What we might know Part II: OG Accounts***

A word about the OG accounts: These are Twitter accounts with one letter (i.e., @B) or a short word (@jack), which are somehow prized in underground hacker forums. In the hours leading up to the Twitter hack, account access for several of these was being offered for as much as \$3,000 per account, according to Krebs and Motherboard.

TechCrunch meanwhile linked this activity to a hacker going by “Kirk,” thanks to a member of an underground forum who told the outlet that this individual was the one behind the spate of account takeovers.

The source said that Kirk claimed to have access to the Twitter admin tool on the company’s network – but that he started out just stealing OG and other “vanity” accounts and selling them on a forum called OGUsers, generating more than \$100,000 in mere hours in the process. TechCrunch obtained screenshots of Discord chats that seemed to verify this.

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

Even with Saturday's update security experts are left to speculate as to what exactly happened and how. Reading through Twitter posts and investigative reports offer up a range of questions: Was SIM-swapping involved? Foreign adversaries? Does @MalwareTechBlog know the true identity of the hackers? Was it a guy named "Kirk"?

"I have been taking press calls all day about this," said Bruce Schneier of Schneier on Security, in a **succinct statement** on Friday. "And while I know everyone wants to speculate about the details of the hack, we just don't know — and probably won't for a couple of weeks."

## Here's at what we do know:

Late Wednesday, a whole cornucopia of high-profile Twitter users fell victim to an attack on Twitter's back end. Tweets sent from those hijacked account read, "I have decided to give back to my community. All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of \$50,000,000."

It's clearly a scam, although the hackers likely hoped that it would look more like a celebrity fad that elites were jumping in on.

It worked to a certain extent; independent researcher Brian Krebs **reported** that the **Bitcoin wallet address** shows 393 transactions worth roughly 12.9 BTC, which is the equivalent of \$118,104.27 using Friday's exchange rate.

Twitter has revealed a few details about what it has uncovered so far and locked down the affected accounts:

**Twitter Support**  @TwitterSupport · Jul 15, 2020 

Replying to @TwitterSupport

Our investigation is still ongoing but here's what we know so far:

**Twitter Support**  @TwitterSupport

We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

Rep. Jim Jordan (R-Ohio), the top Republican on the House Judiciary Committee and a victim in the hacks, asked what would happen if Twitter allowed a similar incident to occur on Nov. 2, a day before the U.S. presidential election, according to Reuters.

Melody Kaufman, cybersecurity specialist at Saviynt, weighed in on this via email.

"I don't think this was entirely a bitcoin scam but instead a proof of concept in which bitcoins were just a side venture," she said. "I think the ultimate goal was to prove that high profile accounts are vulnerable and can be subverted to message on behalf of others. The bitcoin angle serves as a good cover for real motive as it seems to the onlooker that the attackers have gotten what they wanted."

She added, "There are many reasons hackers would want to compromise high-profile social media accounts. Influence has become a form of currency with which a lot of things can be bought. Given that we've already seen the way social media can be used to influence popular opinion and given that this is an election year."

It should go without saying: Until we know the how and who of the Great Twitter Hack of 2020, it will remain unclear as to whether Twitter can adequately address these worries.

Bottom line: There's limited confirmed information on the attack. There are several respected researchers and outlets who claim to have inside hacker sources and good theories (with some evidence) about who's behind the incident. And then there's a fair amount of speculation, uncorroborated theories. For now the best idea is probably, as Schneier pointed out, to wait and see.

***(This article was updated 7/18 at 12:50 p.m. ET with comments from Twitter)***

Write a comment

Share this article:



Cloud Security

Government

Hacks

Mobile Security

Web Security

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE



## Zoom Addresses Vanity URL Zero-Day

An attacker could pose as a company employee, invite customers or partners to meetings, then use socially engineered conversation to extract sensitive information.

July 16, 2020



## Amazon-Themed Phishing Campaigns Swim Past Security Checks

A pair of recent campaigns aim to lift credentials and other personal information under the guise of Amazon package-delivery notices.

July 16, 2020



## Threat Actors Intrigue Unique 'Newbie' Forum

CryptBB becomes more inviting less experienced learn from expert cyber one another.

July 16, 2020

### DISCUSSION

**Anonymous** on July 17, 2020

Twitter could go away tomorrow, and the world would be a better place. Boycott Twitter.

 **Reply**

### Leave A Comment

Write a reply...

Your name

Your email

☐ Save my name, email, and website in this browser for the next time I comment.

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

## ***What we definitely don't know:***

If Krebs' theories and sources are correct, and PlugWalkJoe is indeed the person who masterminded the Twitter hack, it's unclear if his specialty – SIM-swapping – was the initial vector in compromising the company's systems. That's not stopping the Twitterverse from glomming onto the idea, though, including John McAfee, who seemed to lay the blame for the hack at the feet of 2FA and SIM swapping in a Thursday tweet:



**John McAfee**   
@officialmcafee



### THE TWITTER HACK

I may be crazy, but I'm still the founder of the World's largest computer security firm, and I'm telling you:

2 factor authentication is Twitter's worst security threat. It exposes users to the trivial SIM Swap hack, which [@Jack](#) was a victim of.

Wake up Jack!

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE





I'm not a robot

reCAPTCHA  
Privacy - Terms

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

## INFOSEC INSIDER

## Enterprise Data Security: It's Time to Flip the Established Approach

July 16, 2020

1



## Helping Remote Workers Overcome Remote Attacks

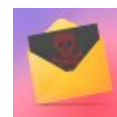
June 10, 2020

1



## Understanding the Payload-Less Email Attacks Evading Your Security Team

June 4, 2020



## Long Tail Analysis: A New Hope in the Cybercrime Battle

May 21, 2020



## The Windows 7 Postmortem: What's at Stake

May 19, 2020

6



Newsletter

### Subscribe to *Threatpost* Today

Join thousands of people who receive the latest breaking cybersecurity news every day.

[Subscribe now](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

[ACCEPT AND CLOSE](#)

your handy guide to the r <https://t.co/62vaKY7NTc>

2:55 PM · Jul 16, 2020



2.6K 915 people are Tweeting about this

Then there's Marcus Hutchins, also known by his online alias MalwareTech, the researcher hailed for squashing the WannaCry ransomware outbreak in May 2017 before **facing criminal charges** over the creation of the infamous Kronos banking malware.

On Twitter, he claimed to have "info leading me to one of the hacker's real identities." He wouldn't offer any further details, but did say to expect "a couple of indictments."

**MalwareTech**   
@MalwareTechBlog

What I love about Twitter is that within 15 minutes of my 1st tweet about the hack, 3 different accounts DM'd me with info leading me to one of the hacker's real identities.

6:33 PM · Jul 16, 2020



3.8K 445 people are Tweeting about this

Another emerging theory, completely unsubstantiated at the time of this writing, is that the hack was carried out at the hands of state-sponsored adversaries.

As one person **tweeted**, in just one of myriad examples: "Trump deliverers a devastating executive order which allows any assets to be stripped from away from anybody helping the oppression of Hong Kong, even in an indirect manner. Less than 24 hours later Twitter has its biggest hack yet. This is China saying: Don't Interfere!"

Certain politicians are also concerned that perpetrators of such attacks could have more nefarious intent – in other words, that the hacks show how easy it would be for U.S. enemies to influence the upcoming election or cause other havoc.

"I'm extremely troubled by this hack of Twitter accounts," Sen. Edward Markey (D-Mass.) said in a **media statement** on Thursday. "While this scheme appears financially motivated and, as a result,

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE

7/19/2020

Twitter Hack Update: What We Know (and What We Don't) | Threatpost

your handy guide to the ... <https://t.co/02ydx1Z1T3>

2 hours ago

Follow @threatpost

191K followers

**Subscribe to our newsletter, *Threatpost Today*!** Get the latest breaking news delivered daily to your inbox.

Subscribe now

## The First Stop For Security News

Copyright © 2020 Threatpost

[Privacy Policy](#)

[Terms and Conditions](#)

[Advertise](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE