TECH / TWITTER / ELON MUSK

Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam / Update: Wednesday's Twitter attack is now being investigated by numerous law enforcement agencies

By NICK STATT / @nickstatt
Updated Jul 16, 2020, 6:41 PM CDT | 0 Comments

Illustration by Alex Castro

The Twitter accounts of major companies and individuals were compromised on Wednesday in one of the most widespread and confounding breaches the platform has ever seen, all in service of promoting a bitcoin scam that earned its creators nearly $120,000.

Multiple law enforcement investigations, including one from the Federal Bureau

of Investigation, are now actively probing the situation over far a deeper concern: that the exploited vulnerability in Twitter's systems — a result it seems of mid-level employees having powerful access to site-wide admin tools that can fall into the wrong hands — has exposed serious security risks for the platform's most powerful users. Lawmakers are hounding Twitter for more transparency around the incident, and it seems likely the attack will have longstanding consequences not just for Twitter's own internal tools and security, but for the broaden cybersecurity industry and every high-profile Twitter user on the platform, too.

We still don't know how exactly the hack happened or even to what extent Twitter's own systems were compromised. But following the unprecedented hacks of accounts including President Barack Obama, Joe Biden, Elon Musk, Bill Gates, Kanye West, Michael Bloomberg, and Apple, Twitter took the drastic step of blocking new tweets from every verified user, compromised or no, as well as locking all compromised accounts.

The Twitter attack has exposed serious security risks for the platform's most powerful users

One notable exception in the attack was the account of President Donald Trump. *The New York Times* is *now* reporting that Trumps's account has special protections in place following past incidents — including when a third-party Twitter contractor used internal company tools to deactivate the president's account in 2017. Those protections may have spared Trump's account from being taken over, although it is not clear right now whether the hackers even attempted to assume control of his account.

Regardless, the national and international security implications of the Twitter attack are now becoming frighteningly clear, as hackers could have caused far more serious damage with access to such high-profile accounts.

Twitter says it won't restore access to their owners "until we are certain we can

do so securely." As of Thursday, the company is still working to restore access to locked accounts, although it has confirmed that no password information was stolen by the hackers in control of the affected accounts, seemingly all of which were verified accounts belonging to high-profile companies and individuals. Twitter says that around 130 accounts were targeted, with the attackers managing to take control of a "small subset" of those. Even some accounts not affected by the attack remain locked, as Twitter continues its investigation. Twitter has not yet disclosed whether private and sensitive direct message threads were compromised as part of the account takeovers; the company says it is "continuing to assess whether non-public data related to these accounts was compromised."

On Wednesday evening, the company revealed that its own internal employee tools were compromised and used in the hack, which may explain why even accounts that claimed to have two-factor authentication were still attempting to fool followers with the bitcoin scam.

The account takeovers have subsided, but new scam tweets were posting to verified accounts on a regular basis starting shortly after 4PM ET and lasting more than two hours. Twitter acknowledged the situation after more than an hour of silence, writing on its support account at 5:45PM ET, "We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly."

The company took the unprecedented measure of preventing verified accounts from tweeting at all starting sometime around 6PM ET. This would seem to be the first time Twitter has ever done this in the company's history. Twitter updated its stance on limiting tweets at 7:18PM ET, writing, "We're continuing to limit the ability to Tweet, reset your password, and some other account functionalities while we look into this. Thanks for your patience." At 8:41PM ET, Twitter said "most" verified accounts should be able to tweet, adding, "As we continue working on a fix, this functionality may come and go."

Late in the evening, Twitter CEO Jack Dorsey wrote, "Tough day for us at

Twitter. We all feel terrible this happened. We're diagnosing and will share everything we can when we have a more complete understanding of exactly what happened." Product chief Kayvon Beykpour also released a public statement on his personal account, writing, "Our investigation into the security incident is still ongoing but we'll be posting updates from @TwitterSupport with more detail soon. In the meantime I just wanted to say that I'm really sorry for the disruption and frustration this incident has caused our customers."

The chaos first began to snowball when Tesla CEO Elon Musk's Twitter account was seemingly compromised by a hacker intent on using it to run a bitcoin scam. Microsoft co-founder Bill Gates' account was also seemingly accessed by the same scammer, who posted a similar message with an identical bitcoin wallet address. Both accounts continued to post new tweets promoting the scam almost as fast as they were deleted, and Musk's account in particular was still be under the control of the hacker as late as 5:56PM ET.

A spokesperson for Gates tells *Recode*'s Teddy Schleifer, "We can confirm that this tweet was not sent by Bill Gates. This appears to be part of a larger issue that Twitter is facing. Twitter is aware and working to restore the account."

Shortly after the initial wave of tweets from Gates and Musk's accounts, the accounts of Apple, Uber, former President Barack Obama, Amazon CEO Jeff Bezos, Democratic presidential candidate Joe Biden, hip-hop mogul Kanye West, and former New York City mayor and billionaire Mike Bloomberg, among others, were also compromised and began promoting the scam.

It's unclear how widespread the operation was, but it appears to have affected numerous major companies and extremely high-profile individuals. That suggests someone, or a group, found a severe security loophole in Twitter's login or account recovery process or those of third-party app — or that the perpetrator has somehow gained access to a Twitter employee's admin privileges. According to *Motherboard*, numerous underground hacking circles have been sharing screenshots of an internal Twitter administration tool allegedly used to take over the high-profile verified accounts. Twitter is now

removing images of the screenshot from its platform and in some cases suspending users who continue to share it.

So far, Twitter has confirmed that employee tools were used in the hack, but not which ones or more than a theory as to how hackers might have gotten access. "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," read a tweet from the company's support account recounting in broad terms how the attack happened, in what was Twitter's first explanation of the incident released Wednesday evening. "We know they used this access to take control of many highly-visible (including verified) accounts and Tweet on their behalf."

1/13

The origin of the scam can be traced to the moment when Musk's account issued a mysterious tweet at 4:17PM ET reading, "I'm feeling generous because of Covid-19. I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!" The tweet also contained a bitcoin address, presumably one associated with the hacker's crypto wallet.

The tweet was then deleted and replaced by another one more plainly laying out the fake promotion. "Feeling grateful doubling all payments sent to my BTC address! You send $1,000, I send back $2,000! Only doing this for the next 30

minutes," it read before also getting deleted. The tweet posted to Gates' account echoed the Musk tweets, with an identical BTC address attached. It was also deleted shortly after posting, only for a similar message to take its place a few minutes later.

Hacked accounts were almost all posting the same bitcoin wallet address

Square's Cash App appears to be one of the other rare company accounts compromised. However, it's not clear if the culprit is the same or if this is some form of a coordinated scam on behalf of a group, as the tweet contained a different BTC address than the ones posted to the other accounts.

In addition to the Cash App, popular crypto Twitter accounts, including those of Cameron and Tyler Winklevoss' Gemini cryptocurrency exchange and widely used wallet app Coinbase, were also compromised. Cameron Winklevoss claims the Gemini account was protected by two-factor authentication and used a strong password, and the company is now investigating how it was hit.

Some people apparently fell for the scam and sent money to the associated BTC address, as records of the transactions are public due to the nature of the blockchain-based cryptocurrency. The scammer amassed nearly $120,000, although it seems as if the account owner is indeed sending money back out as the daily final balance has fluctuated up and down throughout the afternoon, although those accounts may simply be alternative addresses for the same group who perpetrated the attack.

Musk has long been the target of bitcoin scammers on Twitter, many of whom create fake accounts designed to look like the entrepreneur and respond to his tweets promoting the scams so that they appear legitimate. Twitter even went so far as to start locking some accounts that change their name to "Elon Musk," and the company singled out cryptocurrency scammers in spring 2018 as a source of known manipulation and deception that it was aiming to root out through bans

and other moderation strategies.

Update July 15th, 7:33PM ET: *Added new details regarding the Twitter hack and the company's response.*

Update July 15th, 8:53PM ET: *Added that Twitter restored verified accounts' tweeting ability.*

Update July 15th, 11:56PM ET: *Added Twitter's first attempt to explain what happened, including the confirmation that Twitter's own internal tools were compromised.*

Update July 16th, 7:41PM ET: *Added additional details regarding investigations launched into the attack, Twitter's ongoing investigations into how it happened, and the company's attempts to restore access to locked accounts.*

Update July 16th, 11:24PM ET: *Added further details on the extent of the attack.*

JOIN THE CONVERSATION 0

More from this stream **Twitter and the big bitcoin scam: what happened next**

You can now download your Twitter data again and see what hackers could've nabbed

Sep 3, 2020, 4:10 PM CDT

Twitter hack conspirators may include a 16-year-old from Massachusetts

Sep 2, 2020, 12:09 PM CDT

Alleged Twitter teen hacker's hearing got zoombombed big time

Aug 5, 2020, 1:42 PM CDT