Dozens of high-profile Twitter accounts hacked in “coordinated social engineering attack”

Kevin Reed
17 July 2020

Dozens of Twitter accounts belonging to prominent US individuals were breached on Wednesday as part of a coordinated attack aimed at scamming the public out of money in the form of the cryptocurrency Bitcoin.

The compromised Twitter accounts—including those of Joe Biden, Barack Obama, Elon Musk, Jeff Bezos, Bill Gates, Warren Buffett, Michael Bloomberg and Kanye West, along with the corporate accounts of Apple and Uber—sent tweets starting at around 5:45 p.m. EDT, all with similar messages.

For example, the tweet from Joe Biden said, “I’m giving back to the community. All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.” The tweet from Kanye West included, “giving back to my fans” and the one from Elon Musk said, “feeling greatful [sic].”

Several hours after the attack, Twitter Support posted a series of tweets saying, “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.

“We know they used this access to take control of many highly-visible (including verified) accounts and Tweet on their behalf. We’re looking into what other malicious activity they may have conducted or information they may have accessed and will share more here as we have it.

“Once we became aware of the incident, we immediately locked down the affected accounts and removed Tweets posted by the attackers.”

The initial attempts by Twitter to gain control of the situation failed when the company deleted one round of tweets, and they were rapidly replaced by another series by the hackers, indicating that the corporation had completely lost control of its product.

As part of the assault, the hackers also took over the accounts of prominent cryptocurrency leaders and companies earlier in the day. Once this trial, which began at around 4:00 p.m., proved successful, the hackers moved on to the expanded list of politicians and wealthy business and entertainment celebrities.

Later in the evening Twitter disabled the functionality of other “verified” accounts as it scrambled to contain the breach and prevent the Bitcoin scam from spreading. A verified Twitter user is an account holder of public interest, typically journalists, celebrities, professional athletes, government and political figures or business personalities, with a large number of followers such that their identity has been confirmed as authentic. Verified accounts are indicated by a blue badge with a check mark in it next to their Twitter handle.

The support account tweeted, “You may be unable to Tweet or reset your password while we review and address this incident.” Service was reportedly restored to all accounts by 8:30 p.m.

According to a report by CBS News, there were a total of 363 transactions on the Bitcoin account linked to the tweets which “received more than $118,000.” Cryptocurrency exchanges such as Coinbase reported that they were tracking scams being shared on Twitter and working to block transactions from its platform to the addresses that were posted. Another exchange called Binance said that so far none of its users sent funds to the hackers, and it was blacklisting accounts associated with the fraudulent tweets.

Twitter CEO Jack Dorsey commented on the unprecedented hack, “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."

Of particular interest is Twitter's revelation that the hackers successfully penetrated the internal accounts of employees and gained access to "internal systems and tools." According to some reports, access to these tools enabled the hackers to completely bypass account passwords and publish dozens of fake tweets at will.

A report by *Vice Motherboard* claimed that a Twitter insider was behind the operation, citing two anonymous individuals who said they were the hackers who took over the accounts. The Vice report said, "'We used a rep that literally done all the work for us,' one of the sources told *Motherboard*. The second source added they paid the Twitter insider. *Motherboard* granted the sources anonymity to speak candidly about a security incident. A Twitter spokesperson told *Motherboard* that the company is still investigating whether the employee hijacked the accounts themselves or gave hackers access to the tool.

Motherboard also said that the sources provided screenshots of the tool used to hijack the Twitter accounts: "One of the screenshots shows the panel and the account of Binance; Binance is one of the accounts that hackers took over today. According to screenshots seen by *Motherboard*, at least some of the accounts appear to have been compromised by changing the email address associated with them using the tool."

The screenshot published by *Motherboard*, with some user details redacted, shows various functions of the Twitter administrative tool, including details about the target user's account, such as whether it has been suspended, is permanently suspended, or has protected status. Other buttons on the panel include "Bounced," "Inactive," "Compromised," "Trends Blacklist," "Search Blacklist" and "Read Only."

While Twitter has so far neither confirmed nor denied the *Motherboard* report, it did move to remove the tweet which shared the screenshot and suspended the user's account for 12 hours with a message that says the tweet violated company rules. No explanation has been provided as to the purpose of the features of the internal tool, when they are used and on whom they are used.

While the magnitude and damage of Wednesday's hack of numerous accounts through access to the internal systems at Twitter is concerning, the revelation that such tools are being deployed within the social media company, if true, is equally if not more important. Why was it so easy for hackers, once they obtained access to the internal administrative dashboard of the Twitter platform, to manipulate within minutes the accounts of dozens of people and publish statements that they never made?

Cybersecurity expert Alex Stamos, director of the Stanford Internet Observatory and the former chief security officer at Facebook, said that the attacks showed a security flaw in Twitter's service, not lax security by the people who were targeted. Stamos said there were a range of other theories, but all suggested that the attackers got inside Twitter's system, rather than stealing the passwords of individual users. "It could have been much worse. We got lucky that this is what they decided to do with their power," Stamos told the *New York Times*.

The *New York Times* also quoted an unnamed American official, who said that hackers gaining access to Twitter accounts was a "scary possibility" in a world where national leaders, sometimes imitating President Donald Trump's techniques, have adopted Twitter as a primary source of unfiltered communications.

Other US political officials have raised major concerns about the hack, including Senator Josh Hawley (Republican of Missouri) who wrote a letter to Dorsey on Wednesday. Hawley wrote, "I am concerned that this event may represent not merely a coordinated set of separate hacking incidents but rather a successful attack on the security of Twitter itself. As you know, millions of your users rely on your service not just to tweet publicly but also to communicate privately through your direct message service."

Hawley added, "A successful attack on your system's servers represents a threat to all of your users' privacy and data security," and requested that Dorsey work with the Department of Justice and FBI on the matter. He urged Dorsey to respond to a list of questions, including if the attack threatened the security of President Trump's account.