Musk, Obama, Biden, Bezos, Gates—bitcoin scam hits Twitter in coordinated blitz

reader comments

196 with 140 posters participating, including story author

Share this story

Twitter accounts of the rich and famous—including Elon Musk, Bill Gates, Jeff Bezos, and Joe Biden—were simultaneously hijacked on Wednesday and used to push cryptocurrency scams.

As of 3:58 PM California time, one wallet address used to receive victim's digital coin had received more than $118,000, though it wasn't clear all of it came from people who fell for the scam. The bitcoin came from 356 transactions that all occurred over about a four-hour span on Tuesday. The wallet address appeared in tweets from at least 15 accounts—some with tens of millions of followers—that promoted fraudulent incentives to transfer money. At least one other Bitcoin wallet was used in the mass scam.

"I'm giving back to all my followers," one now-deleted tweet from Musk's account said. "I am doubling all payments sent to the Bitcoin address below. You send 0.1 BTC, I send 0.2 BTC back!" A tweet from the Bezos account said the same thing. "Everyone is asking me to give back, and now is the time," a Gates tweet said. "I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

Another variation of the scam promoted a partnered initiative that pledged to donate 5000 BTC to the community and included a domain link to send money. The domain was quickly suspended. This variation came early in the hijacking spree and appeared to affect only cryptocurrency-related businesses, including Binance and Gemini.

Other hijacked accounts belonged to Barack Obama, Mike Bloomberg, Apple, Kanye West, Kim Kardashian West, Wiz Khalifa, Warren Buffett, YouTube personality MrBeast, Wendy's, Uber, CashApp, and a raft of cryptocurrency entrepreneurs. Here's a sampling of some of the scammy tweets:

At 2:58 PM California time, Musk's account continued to pump out fraudulent tweets, despite the mass account hijackings being two hours old. What's more, a screenshot tweeted by a security researcher showed that attackers have changed associated email addresses of some of the hijacked accounts.

That so many social media accounts were taken over in such a short time and remained hijacked for so long is extraordinary if not unprecedented. Previous hijackings that happened to one or two high-profile accounts to promote scams were the result of phishing attacks or the accounts being protected by weak passwords. And in almost all cases, the rightful account holders quickly regained control.

The ability of the attackers to regain control of accounts was also highly unusual. The compromise of so many accounts—many belonging to people who are seasoned in the importance of having good security hygiene—raised serious questions that the compromises were the result of a breach of Twitter's infrastructure.

A Twitter spokeswoman said company personnel are looking into the cause and would respond soon.

A statement Binance issued said its personnel "confirmed that this Twitter breach was not caused by a vulnerability of

Binance’s platform or team members.” The statement didn’t provide any other details about the cause of the hijacking. Binance went on to say: “Our security team has verified that there are zero Binance accounts/users who have sent funds to the hacker’s wallet addresses. The hacker’s wallets are not associated with Binance, and we have prevented all Binance wallet addresses from depositing assets into the hacker’s addresses.”

Emails to some of the other affected account holders weren’t immediately returned.

A spokeswoman for security firm RiskIQ said company researchers were able to track of the infrastructure belonging to the party behind Wednesday’s large-scale hack. So far, they have compiled a list of more than 400 associated domains that included cryptoforhealth.com. the site included in the fraudulent tweet from Binance and other cryptocurrency businesses. Many of the domains didn’t respond, while others led to browser warnings like the one below.

As the hijackings continued, Twitter said that while it investigated, it was suspending the ability of many but not all Twitter users to tweet or respond to tweets. Accounts belonging to verified users were unable to tweet or reply to other tweets. Instead they got a message that said: “This request looks like it might be automated. To protect our users from spam and other malicious activity, we can’t complete this action right now. Please try again later.” The suspension didn’t apply to retweets or direct messages. Unverified accounts worked normally.

This is a developing story. This post will be updated as more details become available.

https://arstechnica.com/?p=1692068