MOTHERBOARD
TECH BY VICE

Hackers Convinced Twitter Employee to Help Them Hijack Accounts

After a wave of account takeovers, screenshots of an internal Twitter user administration tool are being shared in the hacking underground.

By Joseph Cox

July 15, 2020, 6:14pm

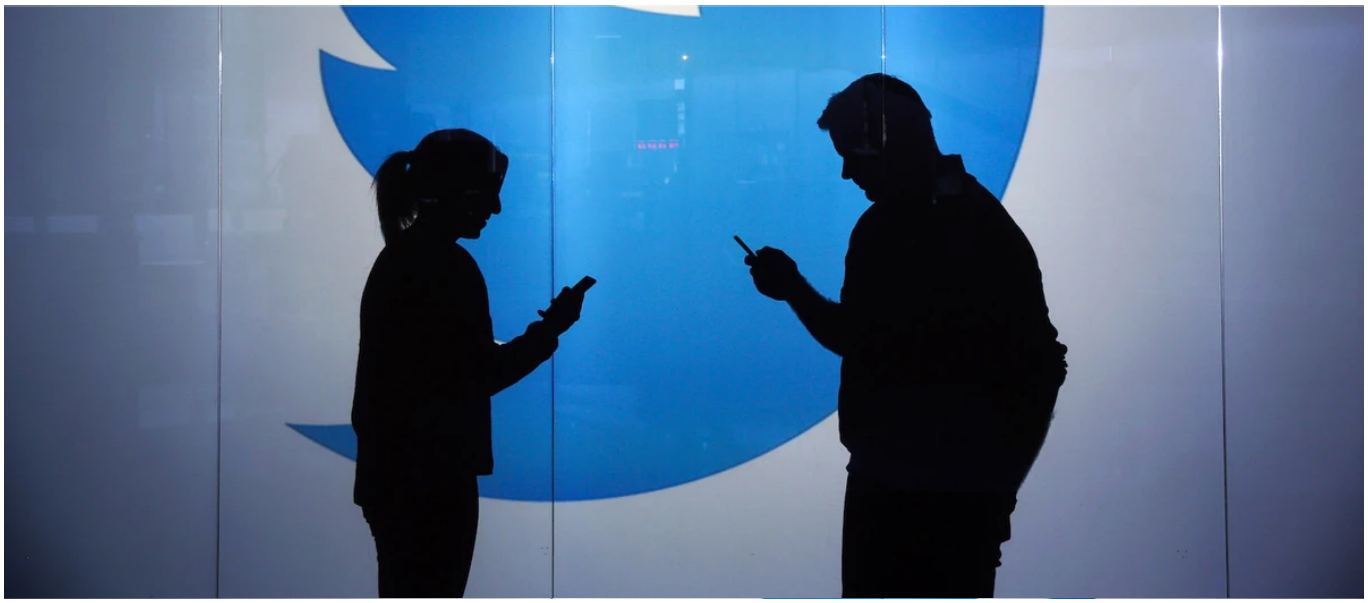

IMAGE: CHRIS RATCLIFFE/BLOOMBERG VIA GETTY IMAGES

A Twitter insider was responsible for a wave of high profile account takeovers on Wednesday, according to leaked screenshots obtained by Motherboard and two sources who took over accounts.

On Wednesday, a spike of high profile accounts including those of Joe Biden, Elon Musk, Bill Gates, Barack Obama, Uber, and Apple tweeted cryptocurrency scams in an apparent hack.

"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. (Update 8/3/20: court documents filed against the suspected Twitter hackers show that one of the hackers who sold access to the ability to take over accounts presented themselves as a Twitter employee to other hackers).

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

sources, as well as screenshots of the tool obtained by Motherboard. 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.

In all, four sources close to or inside the underground hacking community provided Motherboard with screenshots of the user tool. Two sources said the Twitter panel was also used to change ownership of some so-called OG accounts—accounts that have a handle consisting of only one or two characters—as well as facilitating the tweeting of the cryptocurrency scams from the high profile accounts.

Twitter has been deleting some screenshots of the panel and has suspended users who have tweeted them, claiming that the tweets violate its rules.

> **Do you know anything else about these account hijackings, or insider data abuse at other companies? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.**

The panel is a stark example of the issue of insider data access at tech companies. Whereas in other cases hackers have bribed workers to leverage tools over individual users, in this case the access has led to takeovers of some of the biggest accounts on the social media platform and tweeted bitcoin related scams in an effort to generate income.

The screenshots show details about the target user's account, such as whether it

One of the screenshots is a Twitter user posting images of the panel themselves. At the time of writing that account has been suspended.

ONE OF THE SCREENSHOTS OF THE PANEL. ADDITIONAL REDACTIONS BY MOTHERBOARD.

Data breach monitoring and prevention service Under The Breach obtained a similar screenshot and tweeted it as the hackers hijacked several accounts. The person in control of the Under The Breach account told Motherboard Twitter then removed the tweet with the screenshot and suspended them for 12 hours. A message replacing the tweet now says it violated the Twitter rules.

A SCREENSHOT SHOWING THE PANEL'S ACCESS TO BINANCE, ONE OF THE HACKED ACCOUNTS. IMAGE: MOTHERBOARD.

A Twitter spokesperson told Motherboard in an email that, "As per our rules, we're taking action on any private, personal information shared in Tweets."

After the publication of this piece, Twitter said in a tweet 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."

Other hijacked accounts include Mike Bloomberg, and cryptocurrency platforms Coinbase and Gemini. The accounts falsely announced they had partnered up with an organization called CryptoForHealth which claims it was going to provide people with bitcoin as long as they sent some to an address first.

Shortly after the spike of takeovers, Twitter itself tweeted that users may be unable to reset their passwords or tweet while the company addresses the issue.

Within an hour of the breach, Republican Sen. Josh Hawley wrote a letter to Twitter CEO Jack Dorsey asking for more information about the hack, including how the hack occurred, how many users were compromised, and whether the hack affected President Trump's account. Hawley said "please reach out immediately to the Department of Justice and the Federal Bureau of Investigation and take any necessary measures to secure the site before this breach expands."

In 2017, a Twitter worker briefly deleted President Donald Trump's account before it was quickly reinstated.

All tech companies face the issue of malicious insiders. Motherboard has previously revealed how Facebook employees used their privilege access to user data to stalk women; how Snapchat workers had a tool called Snaplion that provides information on users; and how MySpace employees abused a tool called "Overlord" to spy on users during the site's heyday.

Update: This piece has been updated to include a response from Twitter and more information from a SIM swapping source.

Subscribe to our cybersecurity podcast, CYBER**.**

TAGGED: HACKER,TWITTER,INTERNET,SOCIAL MEDIA,UBER,HACKERS,ELON MUSK,COMPROMISE

MORE FROM VICE