# Twitter reveals that its own employee tools contributed to unprecedented hack

Twitter has shed some light on the unprecedented attack on Wednesday that resulted in numerous takeovers of high-profile accounts including those of President Barack Obama, Democratic candidate Joe Biden, and Tesla CEO Elon Musk. In a series of tweets posted this evening under its support channel, Twitter said that its internal systems were compromised by the hackers, confirming theories that the attack could not have been conducted without access to the company's own tools and employee privileges.

"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," the first tweet in a multi-tweet explainer thread reads. "We know they used this access to take control of many highly-visible (including verified) accounts and Tweet on their behalf."

It seems as if Twitter is acknowledging here that numerous people appear to have been involved in the hacks, not just one individual, and also that numerous employees were compromised, too.

> *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.*
>
> *— Twitter Support (@TwitterSupport) July 16, 2020*

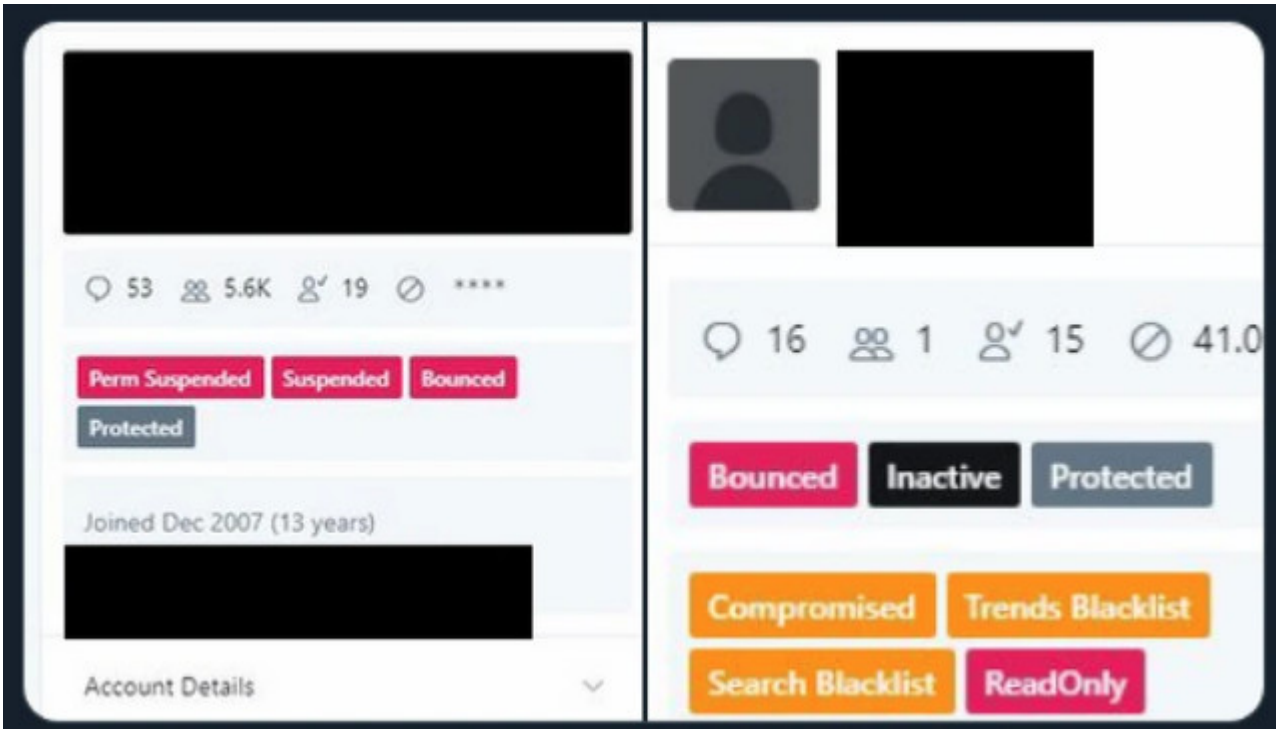
Twitter does not elaborate on what tools the attackers accessed or how exactly the attack was carried out, but *Motherboard* reported earlier today that various underground

hacking circles have been sharing screenshots of an internal company admin tool allegedly used to conduct the account takeovers, potentially by resetting account email accounts and then recovering passwords.

In an update to its investigation on the hack, *Motherboard* now says it's talked to hackers who say they paid a Twitter employee to change the email addresses of popular accounts using the internal tool so that they could then take control of them.

> *we spoke to two hackers and we were able to independently verify they were in control of hijacked accounts today. One of them said they paid the Twitter employee to help them take over accounts; not sure on the specifics here at the moment*
>
> *— Jason Koebler (@jason_koebler)* ***July 16, 2020***

*Motherboard* also shared some of the screenshots of the internal tool allegedly at the center of the hacks, including one here in which *Motherboard* redacted sensitive account info. Twitter is reportedly suspending accounts that share the screenshots and manually removing them for violating its rules.




*A screenshot of the internal Twitter admin tool allegedly at the center of Wednesday's unprecedented attacks that has been circulating among hacker communities, according to* Motherboard.
*Image: Motherboard*

It is not clear if this is definitely how the attack was carried out; Twitter won't say for now. But the near-simultaneous account takeovers of a number of highly sensitive Twitter accounts — including those of presidential candidates and those with two-factor authentication enabled — suggest the attackers did not simply exploit individual account owners and had at the very least indirect access to employee tools.

> *This was disruptive, but it was an important step to reduce risk. Most functionality has been restored but we may take further actions and will update you if we do.*
>
> *— Twitter Support (@TwitterSupport) July 16, 2020*

The company says it's currently investigating "what other malicious activity they may have conducted or information they may have accessed and will share more here as we have it." It's theoretically possible that attackers may have had access to private direct messages, for instance. Those responsible

for the attack appeared to use the account takeovers as a way to promote a bitcoin scam, one that resulted in people sending nearly $120,000 worth of the cryptocurrency to the digital wallet address listed in nearly all of the tweets, blockchain records show.

*Twitter says the hackers targeted its employees for access to internal systems*

But as Twitter alludes to, there could very well have been ulterior motives at play beyond just a cryptocurrency scam, and political and business accounts may have had sensitive information gleaned from those private messages and other account info. Twitter will now likely face serious questions about its internal security precautions and the protections it has in place to prevent this from ever happening again or from resulting in far more catastrophic consequences in the future. It's quite possible Twitter will find itself facing government inquiries and investigations.

Twitter says that once it became aware of the unfolding situation, it "immediately locked down the affected accounts and removed Tweets posted by the attackers." It also took the unprecedented step of disabling the ability for verified accounts to send new tweets.

"This was disruptive, but it was an important step to reduce risk. Most functionality has been restored but we may take further actions and will update you if we do," the update reads. "We have locked accounts that were compromised and will restore access to the original account owner only when we are certain we can do so securely." Twitter also says that it's taken steps internally to "limit access to internal systems and tools while our investigation is ongoing."

https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee-tools