Twitter says hackers used phone to fool staff, gain access

July 31 2020, by Kelvin Chan

In this Wednesday Nov. 6, 2013, file photo, the Twitter logo appears on an updated phone post on the floor of the New York Stock Exchange. Twitter says the hackers responsible for a recent high-profile breach used the phone to fool the social media company's employees into giving them access. The company revealed a few more details late Thursday, July 30, 2020 about the hack earlier this month, which it said targeted "a small number of employees through a phone spear phishing attack." (AP Photo/Richard Drew, File)

Twitter says the hackers responsible for a recent high-profile breach used the phone to fool the social media company's employees into giving them access.

The company revealed a few more details late Thursday about the hack earlier this month, which it said targeted "a small number of employees through a phone spear-phishing attack."

"This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems," the company tweeted.

The embarrassing July 15 attack compromised the accounts of some of its most high profile users, including Tesla CEO Elon Musk and celebrities Kanye West and his wife, Kim Kardashian West, in an apparent attempt to lure their followers into sending money to an anonymous Bitcoin account.

After stealing employee credentials and getting into Twitter's systems, the hackers were able to target other employees who had access to account support tools, the company said.

The hackers targeted 130 accounts. They managed to tweet from 45 accounts, access the direct message inboxes of 36, and download the Twitter data from seven. Dutch anti-Islam lawmaker Geert Wilders has said his inbox was among those accessed.

Spear-phishing is a more targeted version of phishing, an impersonation scam that uses email or other electronic communications to deceive recipients into handing over sensitive information.

Twitter said it would provide a more detailed report later "given the ongoing law enforcement investigation."

The company has previously said the incident was a "coordinated social engineering attack" that targeted some of its employees with access to internal systems and tools. It didn't provide any more information about how the attack was carried out, but the details released so far suggest the hackers started by using the old-fashioned method of talking their way past security.

British cybersecurity analyst Graham Cluley said his guess was that a targeted Twitter employee or contractor received a message by phone asking them to call a number.

"When the worker called the number they might have been taken to a convincing (but fake) helpdesk operator, who was then able to use social engineering techniques to trick the intended victim into handing over their credentials," Clulely wrote Friday on his blog.

It's also possible the hackers pretended to call from the company's legitimate help line by spoofing the number, he said.