Twitter racing to unravel mystery cyberattack

July 16 2020, by Jamie Tarabay, Bloomberg News

Credit: CC0 Public Domain

As Twitter Inc. grapples with the worst security breach in its 14-year history, it must now uncover whether its employees were victims of sophisticated phishing schemes or if they deliberately allowed hackers to access high-profile accounts.

On Wednesday, some of the world's most prominent names, including

former president Barack Obama and Democratic candidate and his former vice president Joe Biden, along with Bill Gates, Elon Musk and Warren Buffett, had their Twitter accounts post invitations for an apparent Bitcoin scam. Twitter reacted by blocking further posts from all verified accounts on the service and said it had detected "a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools."

The company's explanation has ignited speculation over the identity of the perpetrators and what they were actually targeting in the attack. The scale of the endeavor and its timing—months before the November U.S. elections—have given rise among cybersecurity experts to theories that the attack masked a more nefarious campaign to seize sensitive data.

In its investigation of the incident, Twitter will now likely focus on employee logs, email and phone records. At question will be any failures in authentication processes that might have allowed hackers to hijack verified accounts, and also what other information, such as direct messages, might have been compromised in the breach. The Bitcoin wallets promoted in the tweets collected around $120,000 in cryptocurrency.

Twitter shares were down about 6% in pre-market trading on Thursday.

A social engineering attack means "leveraging the human element of security" and there are many different ways to do that, said Rachel Tobac, Chief Executive Officer of San Francisco-based SocialProof Security.

"I can phish someone who has administrative access and try and gain access to their credentials and log into their account," she said, or the less technical method would be to develop "a relationship with someone

who works on those panels and convincing them to do your bidding for you."

Security awareness at companies like Twitter would be mandatory, but ultimately it's hard to track insider attacks when it's the employees rather than the technology who fall under the microscope, Tobac said.

"It used to be the Nigerian prince letter with a bunch of spelling mistakes, and now it's something that almost looks legitimate, but it always starts with a person," said Frances Dewing, the CEO of cybersecurity firm Rubica Inc., based in Seattle.

"There's a playbook for doing this, there are cybercriminal organizations that make millions of dollars. It's the fastest growing business in the world," she said.

And there is no accounting for disaffected workers, as Twitter learned in 2017 when an employee deactivated President Donald Trump's account before it was quickly restored.

Identifying potential Twitter employees to target wouldn't be difficult for the hackers, given the way most smartphone apps hungrily vacuum up location and other contextual data from users—data which is often then sold on to marketing companies. Anyone frequenting the same coffee shops and businesses or entering and leaving a workplace at particular hours can give away clues about themselves.

Cybersecurity experts can only speculate until Twitter itself reveals what happened and where the failures occurred, but even this kind of show of force—a demonstration by hackers to earn credibility or gain infamy—isn't convincing them that a Bitcoin scam was all there was to the operation.

With U.S. elections looming, the cyber landscape is ripe for a major attack. Stas Protassov, co-founder and president of global technology firm Acronis said the attack was "too prepared to be just a cryptocurrency scam."

"We don't believe that's all the hackers went into once they got access," he said in an email. "The attack is too big and too noisy and likely covering a bigger play. We've yet to see the full impact of what this was about."

Tobac also raised the possibility that the attack could have been a distraction while hackers harvested private direct messages and any other confidential data to be able to deploy at a more critical time. So while the initial disruption to Twitter's service appears to have been patched over and the company is gradually restoring normal operation, the lingering effects of this breach might have much wider effects than Wednesday's spectacle.

"Maybe they were doing something insidious and this was just a cover up," she said. "There's no way for us to know, we can just speculate."

Whatever happened, Twitter must be completely candid about the cause of attack once it's established, Tobac said. "This was such a public meltdown that if they're not completely transparent it would damage their brand further."