Bitcoin scam shows Twitter needs better internal controls, expert says

July 17 2020, by Mike Chapple

Credit: CC0 Public Domain

In what appears to be a "coordinated social engineering attack," Bitcoin hackers July 15 took control of dozens of high-profile Twitter accounts, including those of Joe Biden, Barack Obama, Bill Gates, Mike Bloomberg, Jeff Bezos, Elon Musk, and Kanye West, and used them to post messages urging people to send thousands of dollars in cryptocurrency.

The compromised accounts of the politicians, tech executives, major companies and celebrities posted fake tweets offering to send $2,000 for every $1,000 contributed to an anonymous Bitcoin address. Twitter temporarily disabled the accounts and announced "what we believe to be a coordinated attack by people who successfully targeted some of our employees with access to internal systems and tools."

"Schemes like these that use hijacked Twitter accounts to attempt to steal bitcoin are a garden-variety attack that happens every day on Twitter," said cybersecurity and privacy expert Mike Chapple, teaching professor of IT, Analytics, and Operations at the University of Notre Dame's Mendoza College of Business, "But what made this attack unique is that it used stolen accounts belonging to extremely prominent individuals with millions of followers."

Twitter responded quickly and took down the fake tweets, but Chapple says the damage was already done.

"The way that cryptocurrency works, once a transfer takes place, it is irreversible and virtually untraceable," said Chapple, a former computer scientist with the National Security Agency and a former Air Force intelligence officer.

"The simple cash-based motivation of the attackers indicates that they were most likely not nation-state actors," Chapple said. "Another country waging an attack like this would more likely use the access they gained for political or strategic advantage, rather than furthering a simple scam."

Twitter revealed that the attack occurred after one of its own employees fell victim to a social engineering attack where the attackers tricked that employee into granting access to internal Twitter tools.

"One of the functions of those tools is the ability to impersonate another user on Twitter for the purposes of troubleshooting their account," Chapple explained. "It's clear that Twitter's cybersecurity team needs to take a long, hard look at their internal controls to better defend against this type of attack.

"One of the most alarming disclosures made by Twitter last night is that they don't yet understand the full scope of the attack," he continued. "In a late-night tweet, Twitter's support team said that 'We're looking into what other malicious activity they may have conducted or information they may have accessed.' That's quite disturbing, as it indicates that the tweets we saw yesterday might only be the tip of the iceberg for this compromise. Depending upon the nature of the internal tools they accessed, attackers might have compromised other user accounts, gained access to sensitive personal information, or left themselves back doors in the Twitter service that they can exploit at a later date."

Provided by University of Notre Dame