Twitter cryptocurrency scam echoes previous schemes on YouTube

July 23 2020, by William Turton, Bloomberg News

Credit: CC0 Public Domain

The Bitcoin scam that hackers deployed while breaking into the Twitter Inc. accounts of political leaders and business titans last week closely resembles similar schemes used previously on YouTube.

In the July 15 Twitter attack, hackers hijacked accounts belonging to Barack Obama, Elon Musk, Joe Biden and Jeff Bezos and asked their followers to send Bitcoins to their crypto wallet with a promise to double the amount. In a matter of hours, the hackers had accrued more than $100,000.

But before compromising those accounts, the hackers targeted the Twitter accounts of popular cryptocurrency exchanges such as Coinbase Inc., Gemini Trust Company LLC and Binance Holdings Ltd. In this case, the attackers tweeted a link to a website dubbed "CryptoForHealth," which also promised to double donations made to a crypto wallet.

The move caught the attention of computer security researchers, who say similar scams were perpetrated in recent months on Google's YouTube. One of the researchers, who like his colleagues requested anonymity because he isn't authorized to speak publicly, said it isn't yet clear who was behind the Twitter hack but said that the YouTube scams appeared coordinated.

The earlier attacks make clear that stealing user accounts to perpetrate cryptocurrency scams isn't a problem unique to Twitter. The possibility that the incidents are connected may give investigators additional ways to identify the perpetrators, people familiar with the scams say. In online forums, several people have claimed to know the identity of the person behind the CryptoForHealth websites.

One website used as part of the apparent YouTube scams, "btc-gemini.info," looks almost identical to the "CryptoForHealth" site. Beyond the visual similarities, the sites share technical details, such as IP addresses and website code, according to a Bloomberg review of the data.

The links between the schemes on Twitter and YouTube aren't definitive, according to the researchers and Bloomberg's analysis. But at the very least, it shows how easily they can be duplicated, they said.

Alex Joseph, a YouTube spokesman, said the company takes account security seriously by automatically protecting users and notifying them when suspicious activity is detected. "If a user has reason to believe their account was compromised," he said, "they can notify us to secure the account and regain control."

YouTube declined to address whether the alleged crypto scams on its site were related to the Twitter hack. On Tuesday, Apple Inc. co-founder Steve Wozniak filed a lawsuit in state court in California alleging that YouTube has for months allowed scammers to use his name and likeness as part of a phony Bitcoin giveaway.

In the alleged YouTube scams, a hacker typically gained control of an account and made it look like an official page of a cryptocurrency exchange or celebrity. Taking over a YouTube account with an already established following lets the hackers reach a wide audience. That was the same goal with last week's Twitter hack, which hijacked accounts with tens of millions of followers.

After gaining control of an account, the hacker typically live streams an interview with the likes of Bill Gates and runs information about the fake cryptocurrency giveaway alongside it. The alleged scam has been used with video interviews of the Winklevoss twins (who founded popular cryptocurrency exchange Gemini), and Vitalik Buterin, the creator of the Ethereum cryptocurrency.

In June, cybersecurity blog BleepingComputer reported three YouTube accounts were hijacked to run a crypto giveaway scam, this time live streaming an interview with Musk, Tesla Inc.'s chief executive officer,

next to fake information about the scam. In this instance, the perpetrator raked in more than $150,000.

The live streams tend to attract a large audience for the alleged scams before they're detected by YouTube. In some instances, the perpetrators skip stealing an account altogether and simply purchase YouTube ads promoting the alleged scam.

The cryptocurrency company Ripple Labs Inc. filed a lawsuit in April against YouTube over the so-called "giveaway" swindle. "For every scam, giveaway, fake conspiracy that is taken down, multiple more pop up nearly immediately," the company wrote in a blog post. "The reality is that big technology and media companies need to take responsibility and be held accountable for protecting consumers."

In one case, a YouTube user with 282,000 subscribers was hacked and had his account edited to appear as if it was representing the "Ripple Foundation," according to the lawsuit. The attackers then began posting videos from the hacked account promoting the cryptocurrency scam. The user, Mesa Sean, who makes videos of himself playing videogames, didn't respond to a request for comment.

According to the lawsuit, YouTube accounts with hundreds of thousands of followers are targeted with email phishing attacks, where hackers trick the account owner into giving up their password. Ripple estimates that hundreds of thousands of dollars worth of Ripple cryptocurrency have been stolen as part of the illicit operations.

The string of high-profile scams makes it harder for cryptocurrency companies to persuade consumers that their operations are secure.

"Last week's Twitter hack is just the latest dramatic example of an ongoing and widespread problem with social media platforms; malicious

scams on Twitter, YouTube, Medium, Instagram and others have proliferated for years with no real solution," Ripple Chief Executive Officer Brad Garlinghouse said in a statement.

In a motion to dismiss Ripple's lawsuit filed on Monday, lawyers for YouTube said it's not liable for the scams under Section 230 of the Communications Decency Act, which shields platforms from potentially illegal activity by users.