3 charged in massive Twitter hack, Bitcoin scam (Update)

31 July 2020, by David Fischer

The Hillsborough County Sheriff's Office, Fla., released the photo Graham Ivan Clark, 17, after his arrest Friday, July 31, 2020. Clark is accused of hacking Twitter, gaining access to the account of Bill Gates, Elon Musk and many others. Clark was able to scam people around the glove of more than $100,000 in Bitcoin. (Hillsborough County Sheriff's Office via AP)

A British man, a Florida man and a Florida teen were identified by authorities Friday as the hackers who earlier this month took over Twitter accounts of prominent politicians, celebrities and technology moguls to scam people around the globe out of more than $100,000 in Bitcoin.

Graham Ivan Clark, 17, was arrested Friday in Tampa, where the Hillsborough State Attorney's Office will prosecute him as adult. He faces 30 felony charges, according to a news release. Mason Sheppard, 19, of Bognor Regis, U.K., and Nima Fazeli, 22, of Orlando, were charged in California federal court.

In one of the most high-profile security breaches in recent years, hackers sent out bogus tweets on July 15 from the accounts of Barack Obama, Joe Biden, Mike Bloomberg and a number of tech billionaires including Amazon CEO Jeff Bezos, Microsoft co-founder Bill Gates and Tesla CEO Elon Musk. Celebrities Kanye West and his wife, Kim Kardashian West, were also hacked.

The tweets offered to send $2,000 for every $1,000 sent to an anonymous Bitcoin address.

"There is a false belief within the criminal hacker community that attacks like the Twitter hack can be perpetrated anonymously and without consequence," U.S. Attorney David L. Anderson for the Northern District of California said in a news release. "Today's charging announcement demonstrates that the elation of nefarious hacking into a secure environment for fun or profit will be short-lived."

Although the case against the teen was also investigated by the FBI and the U.S. Department of Justice, Hillsborough State Attorney Andrew Warren explained that his office is prosecuting Clark in Florida state court because Florida law allows minors to be charged as adults in financial fraud cases such as this when appropriate. He added that Clark was the leader of the hacking scam.

"This defendant lives here in Tampa, he committed the crime here, and he'll be prosecuted here," Warren said.

Security experts were not surprised that the alleged mastermind of the hack is a 17-year-old, given the

relative amateur nature both of the operation and the hackers' willingness afterward to discuss the hack with reporters online.

"I think this is a great case study showing how technology democratizes the ability to commit serious criminal acts," said Jake Williams, founder of the cybersecurity firm Rendition Infosec. "I'm not terribly surprised that at least one of the suspects is a minor. There wasn't a ton of development that went into this attack."

Williams said the hackers were "extremely sloppy" in how they moved the Bitcoin around.

Williams said it did not appear that the three used any services that make cryptocurrency difficult to trace by "tumbling" transactions of multiple users, a technique akin to money laundering.

He also said he was conflicted about whether Clark should be charged as an adult.

"He definitely deserves to pay (for jumping on the opportunity) but potentially serving decades in prison doesn't seem like justice in this case," Williams said.

Twitter previously said hackers used the phone to fool the social media company's employees into giving them access. It said hackers 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.

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)

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.

Internal Revenue Service investigators in Washington, D.C., were able to identify two of the hackers by analyzing Bitcoin transactions on the blockchain—the ledger where transactions are recorded—including ones the hackers attempted to keep anonymous, federal prosecutors said.

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.

Fazeli's father said Friday he hasn't been able to talk to his son since Thursday.

"I'm 100% sure my son is innocent," Mohamad Fazeli said. "He's a very good person, very honest, very smart and loyal."

"We are as shocked as everybody else," he said by phone. "I'm sure this is a mix up."

Attempts to reach relatives of the other two weren't immediately successful. Hillsborough County court records didn't list an attorney for Clark, and federal court records didn't list attorneys for Sheppard or Fazeli.