

Florida teen charged as “mastermind” in Twitter hack hitting Biden, Bezos, and others



reader comments

148 with 116 posters participating

Share this story

Authorities on Friday charged three people with orchestrating this month’s epic hack of Twitter and using it to generate more than \$100,000 in a bitcoin scam promoted by hijacked accounts of politicians, executives, and celebrities.

Federal prosecutors in San Francisco charged Mason Sheppard,

19, Nima Fazeli, 22, and an unnamed juvenile in the July 15 breach. Prosecutors in Florida, where the juvenile defendant lives, identified him as 17-year-old Graham Ivan Clark and charged him with 30 felony charges. Federal prosecutors said that Sheppard used the hacking names “Chaewon” and “ever so anxious#001” and resides in the UK town of Bognor Regis. Fazeli, who allegedly called himself “Rolex,” “Rolex#0373,” “Rolex#373,” and “Nim F,” is from Orlando, Florida.

The three suspects stand accused of using social engineering and other techniques to gain access to internal Twitter systems. They then allegedly used their control to take over what Twitter has said were 130 accounts. A small sampling of the account holders included former Vice President Joe Biden, Tesla founder Elon Musk, pop star Kanye West, and philanthropist and Microsoft founder, former CEO, and Chairman Bill Gates.

The defendants, prosecutors alleged, then caused the high-profile accounts—many of them with millions of followers—to promote scams that promised to double the returns if people deposited bitcoins into attacker-controlled wallets. The scheme generated more than \$117,000. The hackers also took over accounts with short user names, which are highly coveted in a criminal hacking forum circle calling itself OGusers.

“These crimes were perpetrated using the names of famous people and celebrities, but they’re not the primary victims here,” said Hillsborough State Attorney Andrew Warren. “This ‘Bit-Con’ was designed to steal money from regular Americans from all over the country, including here in Florida. This massive fraud was orchestrated right here in our backyard, and we will not stand for that.”

Painstaking recon, social

engineering, and carefully timed phishing

A security researcher who has been actively working with the FBI on the investigation into this month's breach told Ars that the hack was the result of painstaking research into Twitter employees, the social engineering of them by phone, and carefully timed phishing.

Allison Nixon, chief research officer at security firm Unit 221B, said evidence collected to date shows that Clark and hackers he worked with started by scraping LinkedIn in search of Twitter employees who were likely to have access to the account tools. Using features that LinkedIn makes available to job recruiters, the attackers then obtained those employees' cell phone numbers and other private contact information.

The attackers then called the employees and used the information obtained from LinkedIn and other public sources to convince them they were authorized Twitter personnel. Work-at-home arrangements caused by the COVID-19 pandemic also prevented the employees from using normal procedures such as face-to-face contact to verify the identities of the callers.

With the confidence of the targeted employees, the attackers directed them to a phishing page that mimicked an internal Twitter VPN. The attackers then obtained credentials as the targeted employees entered them. To bypass two-factor authentication protections Twitter has in place, the attackers entered the credentials into the real Twitter VPN portal within seconds of the employees entering their info into the fake one. Once the employee entered the one-time password, the attackers were in.

Nixon and Unit 221B chief legal officer Mark Rasch laid out a description of the hackers' tactics, techniques, and procedures in a post published shortly after the charges were

filed.

ID'd through a hacked database

Prosecutors said they tracked Sheppard and Fazeli through an OGusers forum database that was stolen and published by a group of rival hackers. The database—which the FBI obtained in early April, more than three months before the Twitter hack—contained public forum postings, private messages, IP addresses, email addresses, and other user information of forum participants.

On the day of the Twitter breach, someone with the OGusers account name “Chaewon” advertised that he could change email addresses associated with any Twitter account for \$250 and would give direct access to accounts for for \$2,500 to \$3,000. Chaewon referred buyers to contact the Discourt user ever so anxious#0001.

The OGusers database showed that in early February, a user with the name Chaewon offered to buy a compromised video game account. FBI investigators found that the wallet address that made the payment belonged to the same Bitcoin cluster that ever so anxious#001 used on July 15 to received payments before sending them to an address belonging to Kirk#5270. A Bitcoin cluster is a group of wallets that can be forensically tied to a single individual or entity.

Investigators also used IP addresses Chaewon used to connect to OGusers to tie him to a different OGuser account with the name “Mas,” which was associated with the email address masonshppy@gmail.com. Records investigators got from the Coinbase currency exchange showed that the address was associated with an account owned by a Matthew Sheppard. A drivers license provided by the user of the Coinbase account belonged to Sheppard.

Investigators identified Fazeli when the hacked OGuser

database showed someone with the username “Rolex” proving he had control of a Discord account that was registered to a “Rolex#0373.” In Discord chats that occurred on the day of the Twitter breach, Rolex#0373 had acted as a broker for accounts another alleged hacking participant, with the Discord username Kirk#5270, was advertising for sale.

On OGusers, Rolex also used the email address chancelittle10@gmail.com on multiple occasions in 2018 to receive PayPal payments from other users. The same discussion on Discord showed Rolex#0373 paying Kirk#5270 \$500 for control of the hijacked Twitter account @foreign. Rolex#0373 instructed the address associated with the Twitter account be changed to chancelittle10@gmail.com.

“Charged as adults”

Sheppard is charged with one count each of aiding and abetting intentional access of a protected computer and obtaining information, conspiracy to commit wire fraud, and conspiracy to commit wire fraud. Fazeli is charged with a single count of computer intrusion. Hillsborough County prosecutors, who called Clark the mastermind of the breach, charged him with one count of organized fraud, 11 total counts of fraudulent use of personal information, one count of accessing a computer or electronic device without authority, and 17 counts of communications fraud.

Clark’s prosecution is taking place in Tampa, where he lives, “because Florida law allows minors to be charged as adults in financial fraud cases such as this when appropriate,” Warren’s office said.

<https://arstechnica.com/?p=1695665>