Krebs on security twitter

Detail/Christopher Krebs, director of the Cybersecurity and Infrastructure Security Agency. President Donald Trump has fired Chris Krebs, head of the Cybersecurity and Infrastructure Security Agency, the president announced on Twitter on Tuesday. Krebs' firing is widely expected as Krebs has repeatedly disputed claims that election fraud was responsible for Trump's loss in this month's presidential election. Chris Krebs' recent statement on the security of the 2020 election was extremely false, with rampant impropriety and fraud, Trump tweeted. Trump, without presenting evidence, claimed that dead people were voting, election watchers are not allowed in polling places and errors in voting machines that changed votes from Trump to Biden. In the two weeks since the election, Krebs and his agency have made such energetically disputed claims. The agency set up a rumor control site that lists common fraud claims and then argued they were bogus. For example, it responded to concerns about the turnout of dead people, saying voter registration list maintenance and other election integrity measures protect against illegal voting on the part of dead persons. Please don't retweet wild and unfounded claims about voting machines, even if they were made by the president, ad election security expert David Baker wrote in a tweet last week. Krebs retweeted this tweet from his official CISA Twitter account. Krebs was fully hopeful of his confrontational approach to create friction with the president. Last Thursday, Reuters reported that Krebs expected Trump to fire him. According to Reuters, the White House was pressuring CISA to take down material dismissing fraudulent rumors, but the agency was denied. As it now does regularly, Twitter labeled Trump's tweet announcing Krebs' firing. The claim about election fraud is disputed, the label said. On Monday, dozens of computer security experts signed a letter claiming that hackers had changed the results of the 2020 election. We are aware of the alarming assertions that the 2020 election was rigged by exploiting technical weaknesses, the letter said. However, in every case of which we are aware, these claims have either been unfounded or are technically absurd. To our collective knowledge, no credible evidence has been put forward that supports a conclusion that the 2020 election result in any state has been changed through technical agreement. Twitter was thrown into chaos on Wednesday after accounts for some of the world's most recognizing public figures, executives and celebrities began tweeting out links to bitcoin scandals. Twitter says the attack happened because someone tricked or forced an employee to provide access to internal Twitter administrative devices. Keeping this post out is attempted Of the timeline of the attack, and point to clues about who might be behind it. The first public signal of the intrusion came around 3 p.m. EDT, when the Twitter account for cryptocurrency exchange Binance tweeted a message saying it had partnered with CryptoForHealth to give back 50 bitcoins to the community, with a link where people could donate or send money. A few minutes later, similar tweets went out of the accounts of other cryptocurrency exchanges and from Twitter accounts for Democratic presidential candidate Joe Biden, Amazon CEO Jeff Bezos, President Barack Obama, Tesla CEO Elon Musk, former New York Mayor Michael Bloomberg and investment mogul Warren Buffett. While it may seem ridiculous that anyone would be fooled into sending bitcoin in response to these tweets, analysis of BTC Wallet promoted by several hacked Twitter profiles shows that in the past 24 hours the account has processed 383 transactions and received about 13 bitcoins — or about $117,0 USD. Twitter issued a statement saying it detected a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and equipment. We know that they used this access to take control of many highly visible (including verified) accounts and tweets on their behalf. We are investigating what other malicious activity they have conducted or will share the information they have accessed and more here as we have. There have been strong indications that this attack has been perpetrated by individuals who have traditionally specialized in hijacking social media accounts through sim swapping, involved in providing access to a target account for an increasingly large-scale form of crime that bribes, hacking or forcing employees in mobile phone and social media companies. People within the SIM swapping community are obsessed with hijacking so-called OG social media accounts. Short, OG accounts for the original gangster are usually small profile names (such as @B or @joe). The capture of these OG accounts provides a measure of the situation and perceived impact and wealth in SIM swapping circles, as such accounts can often bring thousands of dollars when res sold in the underground. In the days leading up to Wednesday's attack on Twitter, there were indications that some actors in the SIM swapping community were selling the ability to change an email address tied to any Twitter account. In a post on OGusers – a platform dedicated to hijacking an account – a user named Chaewon advertised they can change the email address tied to any Twitter account for $250, and provide direct access to accounts between $2,000 and $3,000 each. OGUsers Forum user Chaewon is taking the request to modify the email address tied to any Twitter account. This is not a method, you will be given a full If for any reason you are not given the email/email,but if it is revered/suspended I will not be held accountable, Chaewon wrote in his sales thread, which was the title any of the emails for Twitter/Twitter. Hours before any of twitter accounts for cryptocurrency platforms or public figures began blasting bitcoin scandals on Wednesday, attackers have focused their attention on hijacking a handful of OG accounts, including @6. That Twitter account was formerly owned by Adrian Lamo — the now deceased homeless hacker — is perhaps best known for breaking into the Network of The New York Times and reporting Chelsea Manning's theft of classified documents. @6 is now controlled by Lamo's longtime friend, a security researcher and phone phreaker who asked to be identified only by his Twitter surname in this story, Lucky225. Lucky225 said that just before 2 p.m EDT on Wednesday, he received a password reset confirmation code via Google Voice for @6 Twitter account. Lucky said he had previously disabled SMS notifications as a means of receiving multi-factor codes from Twitter, choosing instead to have code once generated by a mobile authentication app. But because attackers were able to change the email address tied to the @6 account and disable multi-factor authentication, the one-time authentication code was sent to both their Google voice account and the new email address added by the attackers. The way the attack worked was that within Twitter's admin tools, apparently you can update any Twitter user's email address and it does so without sending any kind of notification to the user, Lucky told KrebsonSecurity. So [the attackers] could avoid detection by first updating the email address on the account, and then stopped 2FA. Lucky said he hasn't been able to review whether any tweets were sent from his account during the time it was hijacked because he still doesn't have access to it (he's put together the breakdown of the entire episode on this medium post). But almost the same time @6 was kidnapped, another OG account — @B — was swiped. Someone then started tweeting pictures of Twitter's internal tools panel showing @B account. Screenshot of the hijacked OG Twitter account '@B' shows hijackers logging into Twitter's internal account tools interface. Twitter responded by deleting any tweets on its platform that included screenshots of its internal devices, and in some cases the ability of those accounts to tweet further was temporarily suspended. Another Twitter account — @shinji — was also tweeting screenshots of Twitter's internal tools. Minutes before Twitter terminated @shinji account, it was seen publishing a tweet saying follow @6, referring to the account hijacked by Lucky225. Account @shinji Screenshot of Twitter's internal equipment interface. Cached copies of @Shinji's tweets ahead of Wednesday's attack on Twitter are available here and here. Those cash shows Shinji claim ownership of two OG accounts on Instagram-j0e and dead. KrebsOnSecurity is heard from a source who works in security at one of America's largest mobile carriers, who said j0e and dead Instagram accounts are tied to a notorious SIM swaper who goes by the nickname PlugWalkJoe. Investigators are tracking Plugwalkjo as he is believed to have been involved in several SIM swapping attacks in the years before the high-dollar Bitcoin Helist. Archived copies of @Shinji account on Twitter that show one of OG's Instagram accounts, 'Dead.' Now look at the profile image in the second Archive.org index of @shinji Twitter account (pictured below). It was the same image as one wednesday in which @Shinji screenshot was included in which Joseph/@Shinji was tweeting out photos of Twitter's internal devices. Image: Archive.org This person, the source said, was a key partner in a group of SIM swappers that adopted the nickname ChucklingSquad, and was believed to be behind the kidnapping of Twitter CEO Jack Dorsey's Twitter account last year. As Wired.com recalled, @jack was kidnapped after the SIM swap attack against mobile provider AT&T for phone numbers tied to Dorsey's Twitter account by the attackers. In a tweet sent from Twitter CEO Jack Dorsey's account while it was hijacked, Plugwalkjo and other satirical squad members shouted for. The mobile industry security source told KrebsonSecurity that the plugwalk in real life is a 21-year-old named Joseph James O'Connor from Liverpool, Uk. The source said Plugwalkjo is in Spain where he was attending a university until earlier this year. He said Plugwalkjo has been unable to return home due to travel restrictions due to the COVID-19 epidemic. The mobile industry source said Plugwalkjoa was the subject of an investigation in which a female investigator was hired to negotiate with Plugwalkjo and persuade her to agree to a video chat. The source further explained that a video that he had recorded that chat showed a specific swimming pool in the background. According to the same source, the pool pictured on Plugwalkjo's Instagram account (instagram.com/j0e) is what he saw in his video chat with him. If Plugwalko was really pivotal to this Twitter agreement, it's probably fair that he was recognized in part through social engineering. Perhaps we should all be grateful that the perpetrators of this attack on Twitter did not set their sights on the more ambitious purpose, such as disrupting an election or stock market, or attempting to launch a war by issuing false, Tweets from world leaders. Also, it's clear that this Twitter hack could see attackers' direct messages of anyone on Twitter, information that's hard to put a price on, but which would nonetheless be of great interest to a variety of parties, from nation states to corporate spies and blackmailers. This is a fast-moving story. Several people were involved in the Twitter theft. Please stay tuned for further updates. KrebsOnSecurity would like to thank Unit 221B for their assistance in adding some of the dots to this story. Tags: @6, @B, Chaewon, Satirical Squad, Joseph James O'Connor, OG, PlugWalkJoe, Shinji, Unit 221B 221B