GlobalResearch
Center for Research on Globalization

Zombie Seizures: The Hacking of Twitter

By Dr. Binoy Kampmark
Global Research, July 24, 2020
Theme: Intelligence

July 15, 2020. It was a day that will be remembered in the history of social media giant, Twitter.

In what is becoming an increasingly quotidian occurrence with such companies, Twitter faced a hack described as "catastrophic". The company's own language was milder: that day, "we detected a security incident at Twitter and took immediate action." As of July 18, the company believed that the "attackers targeted certain Twitter employees through a social engineering scheme." For the untainted, an explanation is offered. "In this context, social engineering is the intentional manipulation of people into performing certain actions and divulging confidential information." Sounds awfully like Twitter itself.

This internal "social engineering" endeavour enabled the attackers in question to manipulate "a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections." As of that time, 130 Twitter accounts had been accessed and, of them, 45 had their passwords reset. Of these quarried accounts, eight involved the "additional step of downloading the account's information through our 'Twitter Data' tool." (On July 17, the social media giant noted "a lot of speculation about the identity of these 8 accounts" explaining that it would only "disclose this to the impacted accounts". None were verified.)

In responding to the incident, Twitter admitted to being less than forthcoming, "deliberately limiting the detail we share on our remediation steps at this time to protect their effectiveness". Some of these included disabling the means for verified accounts to send new tweets and locking down both affected and unaffected accounts.

> "Most accounts should be able to Tweet again. As we continue working on a fix, this functionality may come and go," Twitter Support announced.

The seized accounts were duly used to spread some fun in what transpired to be cryptocurrency scam centred on a Bitcoin account, though the amount amassed by the scam, being at most $120,000, was modest. The account of Bill Gates, for example, tweeted that, "Everyone is asking me to give back, and now is the time. I am doubling all payments sent to my BTC address for the next 30 minutes." The accounts of former President Barack Obama, Democratic presidential candidate Joe Bien, Jeff Bezos and Elon Musk also figured in the twitter spray.

Those behind the attack do not add up to the customarily sinister portrait of a non-state actor, even if they have sent a chill of tingling discomfort down the spine of the political establishment. The picture, rather, is that of a rabble bound by a petty and rather human objective. A hacker, with the handle "Kirk", secured access to an administrative panel

granting him privileged access to the accounts. Along with other individuals with such uninspired handles as “ever so anxious” and “lol”, compromised Twitter accounts were sold.

This soil, it has to be said, is heavily tilled. Such endeavours were already finding form in the efforts of scammers to impersonate Musk, not merely of Tesla and SpaceX fame but a noted follower of cryptocurrency. Faux accounts of Musk would make offers via Twitter, resulting in the transfer of cryptocurrency. The plausibility of the measure was assisted by bot networks and the occasional reply to a verified account. One such handle was @elomtusk, which, at a pinch, looks rather than @elonmusk. As Marina Coren noted in *The Atlantic*, “This fake account is just one of many in a growing ecosystem of scammers lurking in Musk’s mentions.”

Within Twitter itself, too many fingers, it seemed, were in the security pie. Those fingers, in turn, were unpoliced. This was the opinion of cybersecurity specialist at Saviynt, Melody Kaufmann, who suggested that an unwarranted number within the company had access to verified accounts. Protocols limiting the discretion of any single individual to alter trusted accounts also seemed lacking. “By integrating some measure of cross-checking, it ups the challenge in executing such an attack as it now requires multiple accounts or individuals with privileged access to be compromised at the same time.”

The implications are now being squeezed out of the attack. The fear that verified user accounts risk being hijacked, becoming zombie fronts for the spread of misinformation is gaining some undeserved momentum. The threat is being shaped for the occasion. *Time* wondered whether there was anything to be said about the fact that most of the figures targeted were of the “left”, a rather carefree use of the label. New York Governor Andrew Cuomo preferred to avoid the specifics of the Twitter hack, going straight to the external, interfering bogeyman in announcing a probe. “Foreign interference remains a grave threat to our democracy and New York will continue to lead the fight to protect our democracy and the integrity of our elections in any way we can.” With its 300 million users or so, “Twitter is a primary source of news for many, making it a target for bad actors.”

Senator Josh Hawley of Missouri took it upon himself to send a chastening letter to Twitter CEO Jack Dorsey.

> “I am concerned that this event may represent not merely a coordinated set of separate hacking incidents but rather a successful attack on the security of Twitter itself.” He insisted that Dorsey “reach out immediately to the Department of Justice and the Federal Bureau of Investigation and take any necessary measures to secure the site before this breach expands.”

The FBI duly opened up an investigation into the incident. “At this time, the accounts appear to have been compromised in order to perpetuate cryptocurrency fraud.” Not wishing to miss the investigative boat into the social media behemoth, New York Attorney General Letitia James has also begun an investigation in the name of transparency.

> “Countless Americans rely on Twitter to read and watch the news, to engage in public debate, and to hear directly from political leaders, activists, business executives and other thought leaders.”

The misinformation Cassandras are only accurate to a point. If you believe everything you

see on Twitter, you have embraced the silliest of superstitions. What is factual, let alone truthful, is rarely possible within the intellectually abridged space of a tweet, let alone a vituperative thread. This is a victory for the fearfully shallow.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

---