TWITTER IS ONE HUGE SCAM COMPANY DESIGNED TO PROMOTE ANTIFA EXTREMISM

Twitter Is Crawling With Bots and Lacks Incentive to Expel Them

A researcher finds 1,600 bots tweeting extremist posts in U.S. elections also spread anti-Macron sentiment in France

By
Selina Wang

On Wednesday, the exterior of Twitter's San Francisco headquarters bore an eerie message: "Ban Russian Bots.” Someone— the company doesn’t know who— projected the demand onto the side of its building.

Bots, or automated software programs, can be programmed to periodically send out messages on the internet. Now Twitter is scrambling to explain how bots controlled by Russian meddlers may have been used to impact the 2016 president election.

> "Ban Russian bots" projecting on Twitter HQ right now pic.twitter.com/musk8g085y
>
> — Sean Knox ???? (@smk) October 11, 2017

Investigators hoping to mine Twitter data to figure out who was behind the operation are probably out of luck because the company deleted tweets and other user data, Politico reported today, citing unnamed current and former government cybersecurity officials. The news site said federal investigators now believe Twitter was one of Russia’s most potent weapons in its efforts to tip the election to Donald Trump. Twitter’s privacy policies generally dictate that when a user revises or deletes tweets, paid promotions or entire accounts, the company must do so, too. That data is now almost certainly irretrievably lost, Politico reported.

Twitter was designed to be friendly to bots. They can help advertisers quickly spread their messages and respond to customer service complaints. Research from the University of Southern California and

Indiana University shows that 9 to 15 percent of active Twitter accounts are bots. Many innocuously tweet headlines, the weather or Netflix releases.

After the election, there was little discussion inside the company about whether the platform may have been misused, according to people familiar with the matter who asked not to be identified because it is private. But the ubiquity and usefulness of bots did come up. At one point, there were talks about whether Twitter should put a marking on bot accounts, so that users would know they were automated, one of the people said. Yet most of the conversation after the election focused on whether Trump's tweets violated Twitter's policies, the person said.

The company said it has made a plethora of recent changes, including creating automated processes to detect suspicious logins and stop bad content at its source. Yet experts say that Twitter still lags far behind Facebook and Google.

Twitter executives have been in frequent contact with Congressional committees and investigators to try to answer their questions before hearings on Nov. 1, according to a person familiar with the matter. The company is addressing the issue from multiple angles, the person said, including asking engineers to examine spam use on the platform and asking its business teams to delve into advertising purchases by RT, the Russian TV network.

"As Twitter has grown and evolved in recent years, so has our ability to confront challenges like abuse and harassment. That is why we have invested significantly more resources to improving user trust and safety," a spokeswoman said in an emailed statement. "In addition to establishing a Trust and Safety Council in 2016, we have substantially increased our global staff working on these issues and continue to update our products to foster a safer Twitter." Bloomberg LP is developing a global breaking news network for the Twitter service.

Independent researchers are starting to peel back the layers of political interference. There were about 400,000 bots posting political messages during the 2016 U.S. presidential election on Twitter, according to a research paper by Emilio Ferrara, an assistant professor at the University of Southern California. He told Bloomberg that he has discovered that the same group of 1,600 bots tweeting extremist right-wing posts in the U.S. elections also posted anti-Macron sentiment during the French elections and extremist right-wing content during the German elections this year.

Cybersecurity firm FireEye has previously said that it uncovered thousands of fake accounts linked to Russia that posted anti-Clinton messages. Its examination revealed that on Election Day, one group of Twitter bots sent out the hashtag #WarAgainstDemocrats more than 1,700 times. What FireEye called "suspected Russian bots" caused the hashtag #HillaryDown to start trending, the company said.

Teaching Twitter's algorithms to find malicious tweeters is challenging. Russian meddlers in particular are complementing their networks of bots with human laborers who are paid to Tweet coordinated messages at the same time. It can be difficult for Twitter's algorithms to detect the difference, according to a person familiar with the matter.

And cracking down on bots puts Twitter in a vulnerable position with Wall Street. Investors have penalized the company for failing to get more users. The more that Twitter cracks down on fake accounts and bots, the lower the monthly active user base, the metric most closely watched by Wall Street.

"I think there's a business reason why Twitter doesn't want to be good at it. If you have fake accounts and you're valued around active users, the valuation will be adjusted," said Scott Tranter, partner at Optimus, a data and technology consultancy.

Many Twitter campaigns use bots that automatically retweet any content that comes from certain accounts or that contains certain keywords. Other types of bots are set to reply with pre-written information to tweets that contain specific content.

Kris Shaffer, a data scientist doing research for the University of Mary Washington and the Data for Democracy, found that those strategies were widely used in the lead up to the French election. Many tweets with mentions of LePen or Macron received automatic replies with disparaging information about the candidates.

"The fact they [Twitter] isn't dealing adequately with the propaganda and abuse problems either means they can't do what they say they can do or they can but they aren't telling the truth about the abuse problem," says Shaffer.

Sometimes, activists who are drawing attention to the plague of bots on Twitter become the victim of their attacks. Ben Nimmo, a senior fellow at the Atlantic Council Digital Forensic Research Lab (DFRLab), has found multiple large networks of bots -- with tens of thousands of automated accounts in each -- on Twitter with potential Russian ties. In August, Nimmo worked on Atlantic Council research that was published to show how far-right commentators in the U.S. were using similar narratives to what the Kremlin had been pushing about the Charlottesville attacks.

Shortly after, a long-dormant Twitter account was re-purposed with a profile picture of Nimmo's face -- and a biography saying that he was associated with @KremlinRussia. A second impersonator account was made of the DFRLab's director, which Tweeted that "our beloved friend and colleague Ben Nimmo passed away this morning." That was retweeted over 21,000 times, mostly by bots, according to Nimmo. After Nimmo reported these campaigns, Twitter took down most of the tweets.

Researchers have also found that ISIS used bots to inflate the appearance of support online. The Brookings Institution found thousands of ISIS-supporter accounts using those tactics in 2014.

"The glaring question is: Has the damage already been done?" said Samuel Woolley, research director of the Digital Intelligence Lab at Institute for the Future, a non-profit research organization. "Can Twitter actually even respond to this problem? It's built in a way where it's almost impossible to respond."

Despite all the recent attention, the exact dimensions of Twitter's bot community remains opaque. Academics have asked Twitter to collaborate on research, to no avail, Ferrara, the USC professor, said. He said without internal Twitter data, he cannot figure out the origin and controller of the bots he has

uncovered that posted politically-motivated Tweets. The last time he was in contact with Twitter was after the French elections to follow up on his research and ask the company about how bots were used during the election.

"We interacted many times with Twitter and they always slander our research and say it's methodologically flawed even though we've been consistently right," Ferrara said. "They don't like to collaborate with researchers because then they would receive a lot of bad PR from the type of work that we do." Twitter declined to comment on interactions with researchers.