One in seven Twitter accounts may be nothing more than software 'bots'

August 18 2021, by David Bradley

Credit: CC0 Public Domain

Researchers estimate that one in seven Twitter accounts may be nothing more than software "bots" rather than individuals or organizations using the microblogging platform in an organic manner. A thematic review of this situation is offered by a team from India in the *International Journal of Internet Technology and Secured Transactions*.

Rosario Gilmary, Akila Venkatesan, and Govindasamy Vaiyapuri of Pondicherry Engineering College explain how Twitter bots exploit the service's API (application programming interface) to carry out tasks such as "mentions," "likes," "retweets," and posting updates themselves often exploiting trending topics and "hashtags." Some bots are created for entirely innocent purposes by users but often the bots are created to artificially boost or denigrate the activity of other, legitimate accounts, to spread disinformation, propaganda and other problematic content, and even to spread malware through phishing links embedded in a tweet.

It is important for the service provider and users to be aware of the existence of malicious and unwanted Twitter bots and fake accounts. As such, a review is very timely and might help promote the development of tools to detect these bots. The team discusses in some detail the nature and characteristics of Twitter bots within the following categories based on their activity: fake followers, social spambots, content polluters, and cyborgs. Within the social spambot category, they also identify two other categories of bot: persuasive sockpuppets and progressive sockpuppets.

Within the social bot group, we see the widespread problem of misinformation and propaganda being spread by third parties with the malicious intent to influence unwitting users in their opinions and voting intention in political elections and referenda. It is these Twitter bots that have the potential to have the most lasting and negative effects on society especially when those controlling the bots are rogue actors and even state actors. The team reports that between 9 and 15 percent of Twitter accounts are estimated to be social bots. Worryingly, those who control these bots are well aware of the current detection techniques and evolve better camouflage for their activities in response to defensive measures taken by users and the service provider. It is perhaps an inappropriate cliché to describe the service provider attempts to detect bots and the adaptive bot evolution that is ongoing as a game of "cat and mouse," perhaps it is a game of "cat and bird" given the name of the

service provider and its avian iconography. Either way, the current review points to new ways in which Twitter might identify bots on its system and block or remove them from the platform.

More information: Rosario Gilmary et al, Discovering social bots on Twitter: a thematic review, *International Journal of Internet Technology and Secured Transactions* (2021). DOI: 10.1504/IJITST.2021.116748

Provided by Inderscience