Twitter Bots Detection

Alvaro Albero Gran[1], $DevyaniRaghuwanshi$[1], $KevinStudy$[1], $ShritamaSengupta$[1]
Depart of Computer Science (SEAS)
The George Washington University
Washington D.C, United States of America
(aalbero, draghuwanshi19, kstudy ,shritama33)@gwu.edu

***Abstract*—The social media ecosystem contains bots that are automated and do not require control. These bots can be used either for benign purposes or malicious intent. One social media platform where these bots are rampant is Twitter. This paper discusses the problems with Twitter bots and describes an application that aids the average twitter user in identifying a Twitter bot and taking action to avoid or block it, reducing the bots effectiveness, particularly if the bot is malicious.**

INTRODUCTION

Twitter bots are automated accounts that interact with twitter users, all without any human input. These bots can post content and re-tweet content posted by a user. A bot on twitter re-tweets content from a user and several bots working together can amplify a tweet or hash tag, making it the trending topic on Twitter.

A bot can also tweet original content that includes links or automated responses. Generally, the activity performed by bots is not harmful, but annoying to some and helpful to others. Duo Security, which is now part of Cisco, performed a study on Twitter bots and concluded that these Twitter bots can generate malicious content such as spam or links to websites that may be harmful. Amplify content by re-tweeting original content from a user, hyping its popularity for better or for worse. Perhaps making it trend on social media.

Another report by the Pew Research Center made a similar statement about these types of Twitter accounts. "These accounts can play a valuable part in the social media ecosystem by answering questions about a variety of topics in real time or providing automated updates about news stories or event. At the same time, they can also be used to attempt to alter perceptions of political discourse on social media, spread misinformation, or manipulate online rating and review systems" [1]

. Twitter bots that spread misinformation can affect opinions, especially with regard to elections, not just in the United States but globally. The results can have economic consequences for everyone. It is important that every user be vigilant in policing their Twitter followers for bots that can spread information, but also on followers who are not bots but aid in the dissemination of this false information or malicious tweets. The user must decide whether they want this person or bot following them especially if they re-tweet the misinformation or malicious tweets.

Our group recognizes the hazard that these bots create and created an application that can aid Twitter users in identifying these bots and or suspicious accounts, then use their better judgment about blocking these accounts, limiting their ability to spread disinformation and malicious content. In our paper, our group will describe our application, how it works, and the application will assist users in solving this problem. [2]

RELATED WORK

The dynamics of how users communicate on Twitter make it a fascinating area of both social and security-related study.

A. Types of Twitter Bots

While the classification of Twitter Bots is a very fuzzy one, we can still classify them as good and bad bots. Good bots include the twitter helper bots which help public figures and busy users to automate their tasks like tweeting and posting tweets and images in regular time intervals. These bots are generally used to assist user to save their time from wasting on background user activities that can be simply automated.

Bad bots, on the other hand, can be described as the ones, that similarly automate user accounts as mentioned above but are also responsible to handling thousands.

Sometimes, in case of super bots, millions of user accounts which have no real person behind them. These "non-user" user accounts are then used to increase the follower, like and retweet counts of "real" user accounts who pay enough to the bot engineers to buy them and increase the facet of their twitter profile. Even though, these accounts, have very limited public outreach, buying large quantities of such dead followers can show these user profiles to have high public outreach. Businesses in the look out for influencers with the capacity to publicize their business generally approach such influencers and can end up wasting marketing budget on such fake influencers.

B. Overview of Twitter REST API

Twitter bases its application programming interface (API) off the Representational State Transfer (REST) design. REST engineering alludes to a gathering of system structure rules that characterize assets and approaches to address and access information. The engineering is a plan theory, not a lot of diagrams - there's no single endorsed course of action of PCs, servers and links. For Twitter, a REST design to a limited extent implies that the administration works with most Web syndication groups.

Web syndication is an entirely straightforward idea: An

application assembles data from one source and sends it out to different goals. There are a couple of syndication designs utilized on the Web. Twitter is good with two of them - Really Simple Syndication (RSS) and Atom Syndication Format (Atom). The two configurations recover information starting with one asset and send it then onto the next.
Both Web syndication positions well-suited with Twitter comprise of a couple of lines of code. A Web page administrator can embed it into the code of his or her site. Visitors can subscribe to the syndication service – called a feed – and receive an update every time the administrator updates the Web page. Twitter uses this feature to allow members to post messages to a network of other Twitter members. In effect, Twitter members subscribe to other members' feeds.By allowing third-party developers partial access to its API, Twitter allows them to create programs that incorporate Twitter's services.

There has been some similar work before us that help to evaluate the profile of an influencer. Some of the projects include are:

Botometer, an online web application that indicates the chance a user is real or fake. It is a joint project of the Network Science Institute (IUNI) and the Center for Complex Networks and Systems Research (CNetS) at Indiana University. The output of this application is a meter that checks the activity of a Twitter account and gives it a score based on how likely the account is to be a bot. Higher scores are more bot-like. Below is a screen shot of the Botometer application:

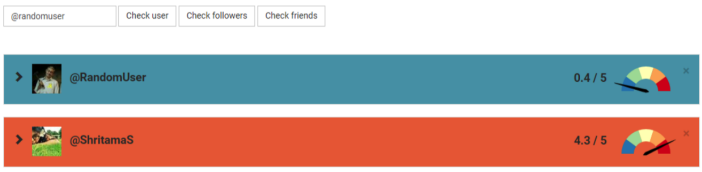

Figure 1. Botometer

Apart from the likelihood of a user being a bot or not, this application does provide a similar measurement of each of the followers of the target user. But other than that, no other user specific information is provided. This poses as an incomplete output since, the viewer or evaluator gets no other information to access the user evaluation and understand the truthfulness of the application calculations.
Another one of the projects that we have looked into while researching for our internal build-up is the Dont@Me, a Duo Labs report submitted by Cisco. This paper details the techniques and tools they created to both build a large dataset containing millions of public Twitter profiles and content, as well as to analyze the dataset looking for automated accounts. By applying a methodical machine learning and data science approach to analyzing our dataset, they were able to build a classifier that effectively finds bots at a large scale.
In this work, they specifically looked for automated accounts, not necessarily malicious automated accounts. Distinguishing benign automation from malicious automation is a topic for future work. They then demonstrated how to pivot off discovered bots to find entire communities of connected bots, or "botnets."
This analysis was given through a case study detailing a large organized crypto−currency spam botnet. They have open sourced their data collection system used to gather account, tweet and social network data to enable the community of security researchers to build on our work. This system allows researchers to quickly build a large Twitter dataset for use in future work.

Methods and Results

To detect and analyze bots and low activity users on twitter there are many features that need to be considered, such as Behavioral and Structural features.

- Behavioral Features: Includes temporal tweeting patterns such as Length of tweets, frequency of tweets,time of tweets etc.
- Structural Features: Includes number of Likes, number of followers, profile image description etc.

To discriminate the bots, fake users, or low activity users from real users several factors were considered in this implemented approach. This is because a single rule or feature may not perform well in differentiating such activities against real users activities. However, according to implemented study it is proven that these factors improved the detection approach if used in combination with each other. Following Classifier Rule-Set we used for implementation of Twitter Bots detection:-

Table I
Classifier Rule-Set

1.	Default Profile Image
2.	Description
3.	The Profile has a name
4.	Friends to Follower Ratio
5.	Number of Followers
6.	Number of Likes per year
7.	Number of Tweets and Re−tweets per year
8.	The account has been Geo-localized
9.	The account has never tweeted
10.	The account name has many numbers is it

- Default Profile Image, Description and profile name: These elements are the most personal of the twitter user. Bots tend to not have changed the default image, do not have a description and the profile name may contain many numbers at the end showing that it has been auto generated.
- Tweets,Number of Likes and Re−tweets these are the structural measures to analyze the user activities. Really high number of tweets and likes in a short period of time are common patterns of bots that are trying to amplify some messages.

- Other parameters such as number of friends and the ratio of friends to followers also help to determine those bots that are simply following many different accounts in order to grow their numbers but they are not followed by anyone because they do not have any real activity or content.

The following figure shows the example of Spam activities on Twitter.Such as duplicate tweets by same user at same time on different days.

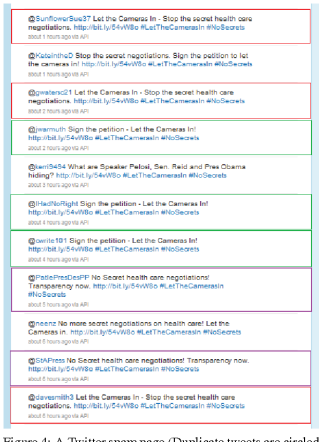

Figure 2. Twitter Spam Page(Duplicate Tweets are circled in a color rectangle)

All these parameters mentioned are analyzed by the algorithm and each of them are given a score based on the predefined weights. All these scores are added up together and based on a threshold it is determined if the user has the explained bot behavior or not. The higher is the score the more suspicious the account is.

Algorithm :Compute_Twitter_Bots

- Step 1: Calculate ratio of number of friends to the number of followers and give score from 0 to 3 based on the value got.
- Step 2: Check if user has a description and set value to 0 or 1.
- Step 3: Calculate score from 0 to 3 based on the number of friends.
- Step 4: Check if user has a default profile image and set value to 0 or 1.
- Step 5: Check if user's profile structure is the default one and set value to 0 or 1.
- Step 6: Check number of tweets per year and give a score from 0 to 3
- Step 7: Check number of likes per year and give a score from 0 to 3
- Step 8: Check how many numbers are in the user name and give a score from 0 to 3.

After doing the calculation of the score for all the categories they are added up and this is the value that is compare to the threshold to determine if the user is real, suspicious or a bot as defined above.

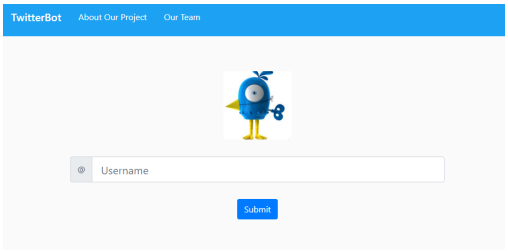

Figure 3. Twitter Bots Detector Front End

The Figure 3 shows the frond end for twitter bots detector. The input value was user name such as 'devyani1904@'. After that, the bots detector fetches the information from the Twitter API and saves it in the data base where the mentioned algorithm is executed and the score for each of the followers is determined.

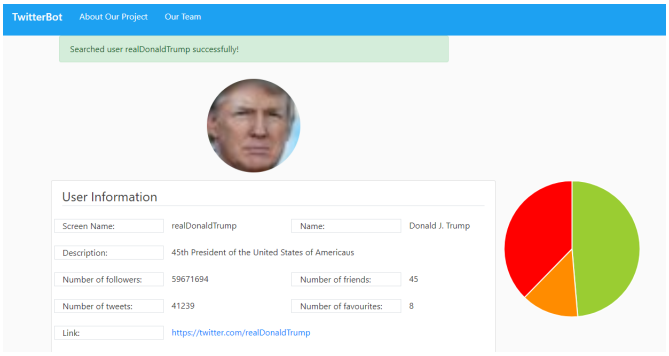

Figure 4. Twitter input User Page (Donald Trump)

As shown in figure, the bots detector gave user information. As mentioned user account has decent number of followers and Friends.Also, the ratio of Followers to Friends was above the threshold value. Other sections such as Description, screen_name etc were also not empty. In order to further investigation of user account, twitter bots detector analyzes the set of followers and classified them into two broad categories such as real user followers and Bots followers.

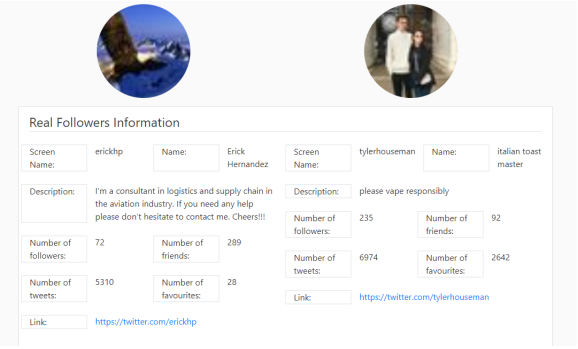

Figure 5. Donald Trump User Account Real Followers Information

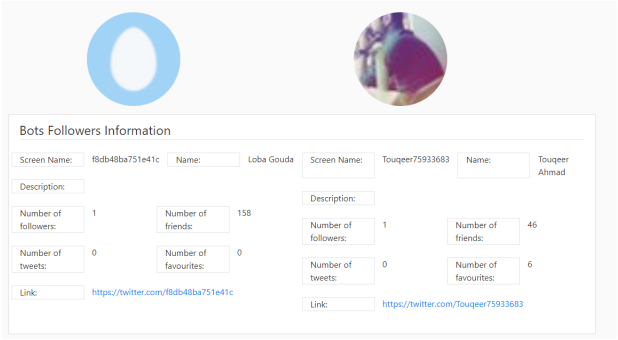

Figure 6. Donald Trump User Account Bots Followers Information

In this way, as shown in figure 2, from our calculations, we can get an approximate idea about the quality of followers of the target Twitter user. We have displayed our results in two parts: 1. The target User Information and an aggregation of follower quality in terms of a pie-chart displaying the percentage of Real, Suspicious and Fake followers. 2. A sample data set of two followers selected at random from each of three categories and display their account details to give the auditor an approximate. Also a link is provided to the different users twitter profile.

Conclusion and Future Work

This developed system is used to detect and report the bots account. We evaluate our method to analyze the user. The evaluation shows how many user followers are real and how many followers have suspicious behavior and how many are bots.

According to research study and results got from the implementation, there are different types of bots with different type of behaviors. This makes a bit more difficult to have an algorithm that is able to classify all of them at the same time that it does not have a lot of false alarms with real users with particular behaviors that can be similar than bots. Future scope includes going deeper in the evaluation and classifying techniques, a machine learning algorithm trained with a set of known bots could give a good result, in order to improve the bot detection tool.

Acknowledgement

Author are grateful to Professor Yih-Feng Hwang for his support, extensive knowledge and kindly teaching.

References

[1] S. Wojcik, S. Messing, A. Smith, L. Rainie, and P. Hitlin, “Bots in the Twittersphere” Pew Research Center, 2018.

[2] O. Anise and J. Wright, “Anatomy of Twitter Bots: Fake Followers” Duo Security, Cisco, 2018.