Think before RT: An Experimental Study of Abusing Twitter Trends

Despoina Antonakaki[1] ✉, Iasonas Polakis[2], Elias Athanasopoulos[1], Sotiris Ioannidis[1], and Paraskevi Fragopoulou ⋆ ⋆⋆[1]

[1] FORTH-ICS, Greece
{despoina,elathan,sotiris,fragopou}@ics.forth.gr
[2] Columbia University, USA
polakis@cs.columbia.edu

Abstract. Twitter is one of the most influential Online Social Networks (OSNs), adopted not only by hundreds of millions of users but also by public figures, organizations, news media, and official authorities. One of the factors contributing to this success is the inherent property of the platform for spreading news – encapsulated in short messages that are tweeted from one user to another – across the globe. Today, it is sufficient to just inspect the trending topics in Twitter for figuring out what is happening around the world. Unfortunately, the capabilities of the platform can be also abused and exploited for distributing illicit content or boosting false information, and the consequences of such actions can be *really* severe: one false tweet was enough for making the stock-market crash for a short period of time in 2013.

In this paper, we analyze a large collection of tweets and explore the dynamics of popular trends and other Twitter features in regards to deliberate misuse. We identify a specific class of trend-exploiting campaigns that exhibits a stealthy behavior and hides spam URLs within Google search-result links. We build a spam classifier for both users and tweets, and demonstrate its simplicity and efficiency. Finally, we visualize these spam campaigns and reveal their inner structure.

Keywords: spam, Twitter, microblogging, social influence, spammer, spam campaign, trending topic, machine learning, classification, regression trees, Gain More Followers campaign, online social networks, privacy

---

⋆ This work was supported by the FP7 Marie-Curie ITN iSocial funded by the EC under grant agreement no 316808

⋆⋆ This work was also supported by the: NSF Grant CNS-13-18415, FP7-PEOPLE-2010-IOF project XHUNTER, No. 273765, Prevention of and Fight against Crime Programme of the European Commission Directorate-General Home Affairs (project GCC), European Union's Prevention of and Fight against Crime Programme Illegal Use of Internet e ISEC 2010 Action Grants, grant ref. HOME/2010/ISEC/AG/INT-002.

1 Introduction

Twitter is one of the most prominent OSNs, characterized as the SMS service of the Internet. This is mainly due to its simple and intuitive design: users are only allowed to post short messages of up to 140 characters. This behavior, also called microblogging, has attracted more than 645 million registered users as of 2014 [19], has over 115 million active users per month with an average of 58 million tweets sent each day and a search engine that performs 2.1 billion queries per day. All this amount of information has established Twitter as a very important service for disseminating the news in our society. Therefore, it is vital that all information originating from Twitter can be practically checked for false (or spam) messages. Consider that about a year ago, a single tweet was enough for making the stock-market crash for a short time [**?**].

But, how can an attacker leverage Twitter? Twitter provides the ability to enrich the semantics of a simple tweet with special characters that prefix specific words. One of the most known prefixes is the hash symbol (#) that denotes a specific word in the tweet as a hashtag. Hashtags are keywords in a tweet that assign context to the entire tweet by associating it with a topic. Even though hashtags started as an intuitive way to categorize and provide context to a message, it became a social phenomenon and their use was adopted by other media (even non electronic) as a simple method to signify, idealize and conceptualize a single word (or phrase) in a short message. Twitter collects popular hashtags and popular search queries and compiles a list referred to as the popular trends, trending topics or, simply, *trends*. Popular trends are becoming part of the social collective memory regarding a specific topic or event. Trends are also dynamic since they change daily and are strongly correlated to a specific location (although some can reach worldwide interest). Unfortunately, trends are a very effective method for tricking users into visiting malicious or spam websites, a technique called *trend-jacking* [12]. According to this, the attackers collect information regarding the most popular (*trending*) topics and include them in tweets pointing to spam sites.

In this paper, we perform a comprehensive study of this phenomenon. Initially we download a large collection of tweets that contain popular trends. Then we extract the contained URLs and we measure the number of contained trends as well as other features. We use 86 different Real-time Blackhole Lists (RBLs) to obtain the spam status of the collected URLs. We refer to this class of spam as *RBL*.

We also identify a specific type of spam campaigns that evade detection by masquerading URLs as Google search results. Spam campaigns are orchestrated, with large amounts of tweets coming mostly from hijacked accounts [8] that are promoting a specific service or product. These campaigns attempt to attract victims by offering to increase the number of accounts that follow the user. We refer to this class of spam as *GMF* (Gain More Followers). These campaigns are propagated with the following technique: They trick users into giving permission to a malicious website, e.g., by trusting a site that advertises some type of meta-analysis of the user's account. Usually these fraudulent services offer to

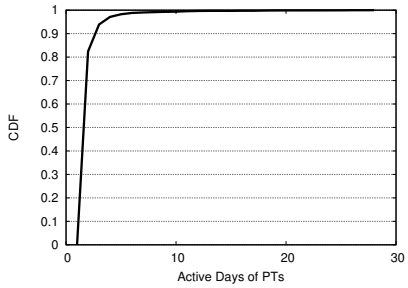
report usage statistics, analysis on user's followers, which followers retweet most of the user's tweets or who viewed the user's profile. Interestingly, most of the services that these sites offer can actually be performed without giving any special permission to the third-party. Even more surprising is the fact that there are legitimate sites that perform most of this analysis, for example: [1]. This points to the fact that there is a serious lack of public awareness regarding the actions that third-party services can perform when explicit authorization is permitted, as opposed to what actions can be performed by simply accessing a user's public data. Moreover, either as a paid service or a free one, these "get-more-followers" campaigns [17] consist a serious threat since it is a multi-million dollar scheme [15]. Our analysis shows that spammers propagating these campaigns follow a stealthier approach (compared to other spammers) as it hides URLs redirecting to spam sites within Google search results links. From all the Twitter features we study, the amount of different popular trends, included by a user in tweets, exhibits the highest divergence between spammers and legitimate users.

Based on our findings, we build a classifier that uses these features to differentiate between spammers and legit users. Our classifier on GMF class spam, is able to achieve a True Positive Rate (TPR) of 75%, which is comparable to existing studies, while maintaining a False Positive Rate (FPR) of 0.26% that is significantly lower than existing studies. We also extend the classifier to focus on individual tweets rather than users with similar results (79.6% TPR and 0.77% FPR). We also demonstrate the efficiency of our technique that requires minimal computational effort, as it takes advantage of Twitter-provided features with minimum pre-processing. Finally we visualize the GMF campaigns and reveal that, while all spam domains originate from only 2 IPs, they are posted by thousands of users.

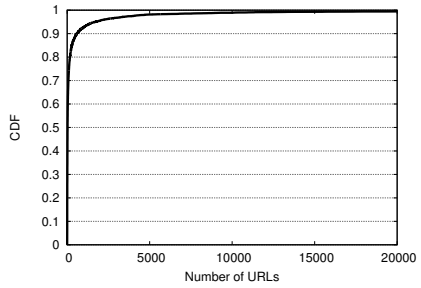
2 Background

A natural consequence of Twitter's rapid growth was to become a very popular medium for deploying spam campaigns [11]. Furthermore, Twitter's architecture facilitates the rapid propagation of phishing and spam attacks [9]. As a first line of defense, Twitter has employed a URL shortener service that preemptively checks for reported malware and phishing sites before shortening a URL [2]. With this defense spam in Twitter has reportedly dropped to 1% [3]. Additional studies have suggested methods for feature extraction from tweets and application of machine learning methods for spam identification. The main requirements when developing these techniques are high TPR, low FPR, simplicity and low computational requirements [13, 14, 9].

The analysis pipeline followed in most existing studies starts by extracting various features from tweets. These features can be either content based [20, 10, 4, 5, 12] or graph based [20, 10, 4, 5]. Some studies analyze specific spam strategies [16]. Then they proceed to flag (or label) the tweets or user in order to form a ground truth. Techniques to do that are: manual inspection [20, 5, 6],



(a) Prevalence of PTs for March of 2014.



(b) Number of different URLs associated with a specific trending topic.

Fig. 1

consult online blacklists [12, 4], honeypots [10] or delegate this task to Twitter itself via the embedded URL shortening service [4, 7]. Then they proceed to train a Machine Learning algorithm to classify either users [20, 10, 4–6] or individual tweets [20, 5] between spam and legit categories. They employ various algorithms such as Naive Bayesian [20], Decision Trees [12, 7], Random Forrests [10], Support Vector Machines [5], Aggregate methods [4] and web search [6]. Some studies also perform Unsupervised learning (clustering) [4, 7].

It is in general difficult to perform comparisons between existing studies, since they measure different features and they follow diverse analysis pipelines. In general best studies are considered the one that achieve True Positive Ratio (TPR) higher than 80% and False Positive Ratio (FPR) lower than 1%. In our implementation, we demonstrate how we can achieve similar classification results, with simpler and computationally lighter techniques while relying on separate features that can lead to a previously undetected set of spam campaigns.

3 Methodology

Twitter has released a public API for interacting with the service. Through this API we collect daily Popular Trends (PTs) and tweets that contain these trends. Subsequently, since all URLs are automatically shortened by Twitter, we apply a URL expansion process that allows us to collect the final URL that is contained within each tweet. On average we downloaded 240 PTs per day and 1.5 million tweets. Our data collection phase lasted for three months, specifically January—March of 2014, during which we collected 150 million tweets.

In Figure 1a we show how prevalent certain PTs were during March of 2014. We can see that 80% of the trends are active for 2 days or less. However, certain trends remain active and very popular for more than 20 days.

Another interesting observation is the different number of URLs posted per trend. In Figure 1b we plot a CDF of the number of different URLs associated

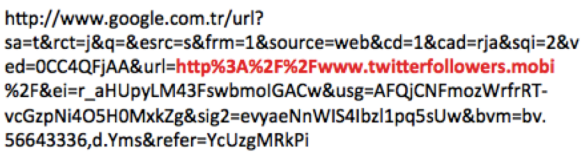


Fig. 2: An example of a get-more-followers spam link camouflaged as a Google search result.

with a particular popular topic. We observe that approximately 90% of trends are associated with less than 10,000 URLs.

3.1 Feature Extraction

The next step was to extract various user metrics, that will be used as *features* for our classifier. For each user we collected: The total number of tweets, the number of Total and Unique Popular Trends, Hashtags, User Mentions and URLs, the number of followers and the number of followings.

Grouping potential spam campaigns. After calculating these metrics, we build a graph containing the users and group them according to the URLs they sent, i.e., creating subgraphs for each URL that contain all the users that included it in a tweet. Since we are interested in URLs that are posted in bulk, we extract all link nodes that have a degree smaller than 10. Subsequently we collect the domain name of each URL. This results in the collection of 24.000 different domain names during our 3 month collection period. Next, we attempt to obtain the ground truth by identifying which URLs belong to spam domains. We follow two methods for obtaining that information. First, we utilize various blacklists and, second, we employ a heuristic to identify spam that belong to the GMF class.

3.2 Real-Time Blackhole Lists (RBL)

Initially, we query various Real-Time Blackhole Lists (RBLs) to identify spam campaigns contained within our dataset. The advantages of RBLs is that they offer a fast and low-bandwidth method for spam detections. The main disadvantage, however, is that they exhibit delays for updating and including new spam domains [9]. For our experiments we used 86 RBLs.

3.3 Get-more-followers (GMF) campaigns

During the manual inspection of the collected URLs, we observed a large percentage that appeared to be Google search results. Finding Google search results URLs within Twitter can be simply attributed to the following scenario: users that copy URLs from a Google search results' page and paste them into a tweet. Even though these URLs appear in the browser to be from domains other than

Google, when copied they actually are Google URLs. When clicked, Google redirects the user to the desired link but, first, records the fact that this specific user clicked this link. After a more detailed inspection, we found that spammers exploit this and use it as a mechanism for *link obfuscation*. We present an example of such a case in Figure 2. Thus, spammers are able to masquerade spam URLs as Google results and conveniently bypass any blacklists or filtering mechanisms. We collected all Google results URLs from our dataset and identified 44 domains belonging to the get-more-followers (GMF) domains. We subsequently searched in RBL blacklists for domains that contained the word "follow" and we enriched this list with another 62 domains. These 106 domains mapped to 33 different IP addresses.

4 Data Analysis

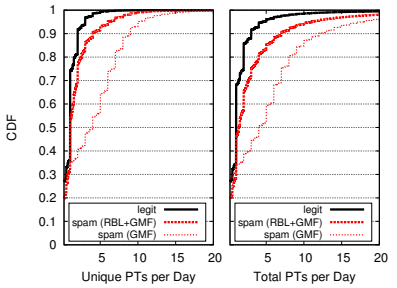
In this section we present the results from our analysis of collected data, following the methodology presented in Section 3.

Using the list of 86 blacklists and our GMF heuristic, 1,911 domains from our dataset were flagged as spam, accounting for 7.9% of all the checked domains. These 1,911 domains traced back to 1,429 different IP addresses. After manual inspection we removed 91 domains that were obvious false positives. Surprisingly, we found that out of the 4,593,229 different URLs that we collected during March of 2014, 250,957 pointed to a single spam domain. This is 5.4% of all URLs, which is significantly higher that the 1% that Twitter reports [3]. This demonstrates that a notable amount of spam is able to bypass Twitter's spam detection mechanism.

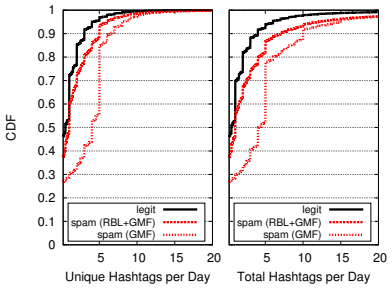
Having acquired a significant labelled dataset of spam URLs, we proceed with identifying all spam users by examining which users posted spam URLs. From a total of 8.2 million users, we locate 590,000 that have posted at least one spam link which accounts for 7.2% of the users. As we mentioned in Section 2, these users are most likely victims whose accounts have been compromised rather than being spammers themselves.

The next step is to examine the features we have collected and see how different they are for spammers (including compromised accounts) and legitimate users. Our results show that all metrics exhibit a larger mean value for spam users compared to legitimate ones. Among them, Total Trends and Total Hashtags exhibit the highest mean increase, (2-fold). We also observe that the Different Trends and Different Hashtags exhibit similar average increases (both from 1.0 to 1.6) This is expected given the similarity of these two features (PTs and Hashtags). Moreover the difference of the average values for Twitter features between spammers and legitimate users is wider in the case of the GMF domain dataset. Surprisingly, we don't observe any significant difference for the number of User Mentions compared to the RBL+GMF dataset. This leads us to the conclusion that this feature is not exploited by spammers.

Having identified the features that present the largest divergence between legitimate users and spammers, we continue with plotting the distribution of



(a) CDF of Popular Trends of users weighted by the number of Active Days.



(b) CDF of Hashtags of users weighted by the number of Active Days.

Fig. 3

users for each of those features. Figure 3a presents the distribution of PTs for legitimate users and spammers. The left subplot contains the unique PTs per day and the right one, the total PTs per day. We plot two different sets of spammers; one for both the RBL and GMF datasets and one for the GMF alone. We follow the same approach in Figure 3b that contains the distribution of Hashtags. The two figures demonstrate the extent to which spammers exploit the PTs and Hashtags for promoting their campaigns and reaching as many users as possible. A key observation is that the unique Trends and unique Hashtags exhibit higher differentiation than the total Trends and total Hashtags. Thus, spammers incorporate a large number of different trending topics so as to show up in various user queries and achieve a larger coverage and more diverse set of users, while maintaining a constrained approach to the total number of hashtags tweeted in a day. That is an indication of spammers following a stealthy approach and not flooding the system, to avoid being flagged by Twitter's spam detection mechanism. This confirms our initial intuition that posting many different trending topics is more suspicious than just posting many tweets containing trending topics. Moreover, we notice that GMF spam is far more active in exploiting PTs and Hashtags compared to RBL.

5 The Classifier

In this section we describe the classification schema that we used as a mechanism to discriminate between spam and legit users. Each user has a class information that is defined as the average number of spam tweets per active days. This metric indicates not only if a user is a spammer or not, but also the level of spam activity that he/she exhibits. The next part was to split the dataset into two random subsets. The first was used to train the machine learning algorithm and the second was used as a test dataset in order to assess the predictive ability of the model. We used a random 90% of the initial dataset as train and the remaining 10% as test.

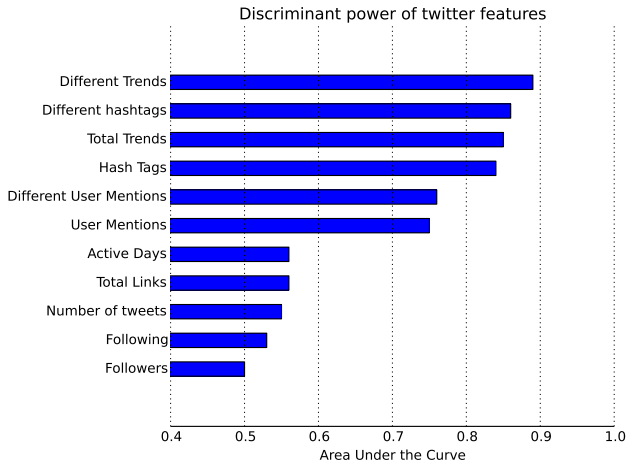


Fig. 4: The Area Under the Curve (AUC) metric for each feature.

After the construction of the train and test datasets we train a Decision Tree Regression (DTR) classifier. This method takes advantage of the rich information that is conveyed in the class feature (average number of spam tweets per active days). After training the DTR model, we assess the TPR and FPR metrics of the classification on the test dataset. We repeat this procedure 100 times. Each time we construct a novel train and test dataset as presented above, we train a DTR and assess the TPR and FPR metrics. Finally we report the average TPR and FPR metrics. This approach is called repeated random sub-sampling validation. We used the python package scikit-learn to train and assess the DTR classifier.

We applied this classification schema on tweets collected throughout March 2014. This collection contained 622,428 users from which 5,152 have posted at list one GMF spam tweet. These users have posted in total 6,658,2825 tweets. The average TPR was 75.1% and the average FPR was 0.26%. Finally we performed an analysis of the dicriminatory ability of each feature. We did this by measuring the performance of the classification scheme when we apply only one of each feature and we blind the rest. Then we measured the Area Under the Curve (AUC) of the Receiver Operating Characteristic (ROC) plot of the trained model. An AUC equal to 1.0 indicates a perfect classifier, whereas 0.5 indicates that the model does not perform better than a random classifier. This analysis show that both total and different trends and hashtags perform good as features for spam detection (Figure **??**).

5.1 Tweets classification

In this section we present the ability of the features to discriminate individual tweets that belong to the GMF campaigns. In this experiment every tweet that does not belong to the GMF campaign was assigned a negative class. We

used again the tweet collection from March 2014 which contains 63,612 tweets belonging to the GMF campaigns (out of 6.6 million). The features that were extracted for each tweet were: Total Links, Hash Tags, User Mentions, Retweet Status, and Total Trends. We applied the same learning and validation schema as in the user classification experiment. The only difference is that we applied a Decision Tree Classifier (DTC) instead of a DTR. DTC is more applicable to this task since we are facing a binary classification problem. The average TP rate of the classifier was 81% and the average FP rate was 0.18%. In comparison, [7] succeeded 55% TPR and 0.4% FPR on twitter data and 80.8% TPR and 0.32% on Facebook data. Of course identifying spam that belong in the GMF campaign is a relatively easy task since it is based largely on hijacking of trending topics.

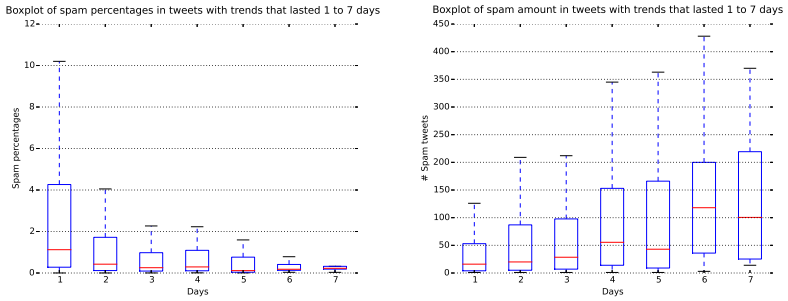
In decision trees the most discriminant rule is located on the root node. In our case this rule was: if Total_Trends <3.5 then legit else spam. This single rule has 79.6% TPR and 0.77% FPR. Practically this means that just by checking the number of Trends in a single tweet, an algorithm can identify 4 out of 5 tweets that belong in the GMF campaign.

5.2 Time scale analysis of Popular Trends

We also analyzed the time period that is usually takes before a Hashtag is exploited after it becomes a PT. During March of 2014 we collected 5,780 different PTs. From these 3,193 (55%) had been used in at least one spam tweet. The 74.5% of these trends where involved in spam tweets for only a single day and 15% for two days. This show that the vast majority of PTs are exploited the very first days that they are created. Since acquiring a list of PTs from Twitter is an easy task, spammers seem to do this daily in order to add them on spam tweets. In figure 4a we present the boxplots of spam percentages in tweets containing PTs that lasted from 1 to 7 days. Trends that lasted more than 7 days were very few (<1%) and were excluded from our analysis. It is impressive that 1% of tweets that contain trends that are active only for a single day is spam. We also observe a downward trend, meaning that PTs that are active for more days contain a lower percentage of spam. Nevertheless if we repeat the same plot with the absolute number of spam (rather than percentages), we observe an upward trend (figure 4b). This means that PTs that are active for more days contain a higher amount of spam. As we have seen PTs that are active for more days are more generic, thus they are exploited in a higher level. Nevertheless targeting PTs with shorter duration is more effective since it is exploiting novel trends and potential unsuspicious users.

6 Spam campaigns

As we have previously discussed, in most cases spam delivery happens on a massive scale with well orchestrated behavior [18]. To further illustrate this, we plot a recreation of a spam campaign that was captured on a single day (January 10^{th} 2014) in Figure 5. This campaign comprised of 17 different spam domains



(a) Boxplot of spam percentages. (b) Boxplot of absolute spam amount.

Fig. 5

belonging to the GMF class, which involved 1,604 different users. 16 out of these 17 domains belong to a single IP address. This IP also hosted 2 more domains that were contained in the blacklists, but that did not take part in this campaign. The average edge degree for a node that represents a spam domain is 125, i.e., every spam domain in the graph could be found in average, in the tweets of 125 different users. In contrast, the average edge degree for the graph depicting users and the URLs they tweeted for that day, is 2.3 for legitimate URLs. Various graph properties can be exported either from spam campaign graphs, or user-URL graphs, that can potentially assist in identifying spam users and campaigns. We plan to explore this as part of our future work.

The most successful domain is tweeted by 337 users, while the least by 40. These numbers demonstrate the stealthy approach of this type of campaigns that do not flood Twitter with multiple messages advertising the campaign, which would result on being detected by Twitter's spam detection mechanism. The average number of tweets per user ranges from 1.07 to 1.58, meaning that in the worst case only half the users will promote the spam domain a second time.

7 Conclusions

As the impact of Online Social Networks (OSNs) becomes more prominent in modern societies, it is crucial to study the emergent patterns of both benign and malign user behaviors. In particular, spam distribution can be disruptive for the finances and the privacy of individual users. For this reasons delving into the methods and techniques employed for spam distribution is essential for protecting users and uncovering potential system vulnerabilities.

In this paper we conduct a study regarding the characteristics of spam propagating through Twitter and, specifically, how spammers use certain features of the service to increase the effectiveness of their campaigns. Our exploration of our 3-month dataset revealed a set of spam campaigns that exhibited a stealthier approach than other campaigns and also masqueraded URLs pointing to spam

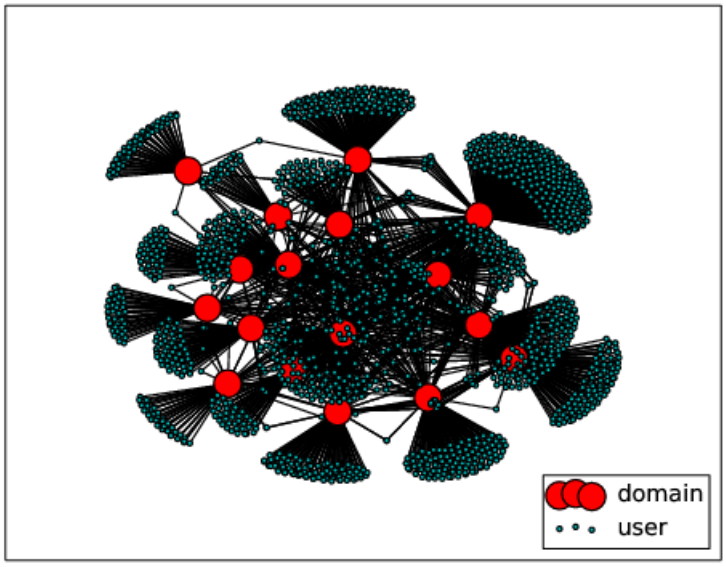


Fig. 6: Plot of a spam campaign involving 17 GMF domains and 1.604 users

websites as a Google search result. Using a set of 86 blacklists, and a heuristic for identifying these new campaigns, we create labelled datasets that we use for training a classifier. We then quantify the behavior of legitimate users and spammers using metrics for Twitter-specific keywords and content, and find a large divergence in categories such as the number of trending topics included in tweets.

We create a classifier for a spam detection mechanism that uses these metrics, and test it on a dataset containing all the tweets collected during a period of one month. Our detection mechanism is able to correctly identify 75% of the stealthy spammers, while maintaining a very low false positive ratio of 0.26%. Overall, our system offers a light detection mechanism for a stealthy and persistent class of Twitter campaigns, while maintaining a very low false positive rate that is a very significant requirement for deployment in a real environment. It also relies on features that require low to zero computational resources since they are widely available from Twitter's API.

References

1. `http://followerwonk.com/`.
2. `https://blog.twitter.com/2012/shutting-down-spammers`.
3. `https://blog.twitter.com/2010/state-twitter-spam`.
4. Amleshwaram, A. A., Reddy, A. L. N., Yadav, S., Gu, G., and Yang, C. Cats: Characterizing automation of twitter spammers. In *COMSNETS* (2013), IEEE, pp. 1–10.

5. Benevenuto, F., Magno, G., Rodrigues, T., and Almeida, V. Detecting spammers on twitter. In *Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)* (2010).
6. Flores, M., and Kuzmanovic, A. Searching for spam: detecting fraudulent accounts via web search. In *Passive and Active Measurement* (2013), Springer, pp. 208–217.
7. Gao, H., Chen, Y., Lee, K., Palsetia, D., and Choudhary, A. Towards online spam filtering in social networks. In *Symposium on Network and Distributed System Security (NDSS)* (2012).
8. Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., and Zhao, B. Y. Detecting and characterizing social spam campaigns. In *Proceedings of the 10th Annual Conference on Internet Measurement* (2010), ACM.
9. Grier, C., Thomas, K., Paxson, V., and Zhang, M. @spam: The underground on 140 characters or less. In *Proceedings of the 17th ACM Conference on Computer and Communications Security* (New York, NY, USA, 2010), CCS '10, ACM, pp. 27–37.
10. Lee, K., Eoff, B. D., and Caverlee, J. Seven months with the devils: A long-term study of content polluters on twitter. In *ICWSM* (2011).
11. Markatos, E., Balzarotti, D., Almgren, M., Athanasopoulos, E., Bos, H., Cavallaro, L., Ioannidis, S., Lindorfer, M., Maggi, F., Minchev, Z., et al. The red book.
12. Martinez-Romo, J., and Araujo, L. Detecting malicious tweets in trending topics using a statistical analysis of language. *Expert Syst. Appl. 40*, 8 (June 2013), 2992–3000.
13. O'Donovan, J., Kang, B., Meyer, G., Höllerer, T., and Adalii, S. Credibility in context: An analysis of feature distributions in twitter. In *SocialCom/PASSAT* (2012), pp. 293–301.
14. Ozdikis, O., Senkul, P., and Oguztuzun, H. Semantic expansion of hashtags for enhanced event detection in twitter. In *Proceedings of the 1st International Workshop on Online Social Systems* (2012).
15. Perlroth, N. Fake twitter followers become multimillion-dollar business. *The New York Times* (2013).
16. Sridharan, V., Shankar, V., and Gupta, M. Twitter games: How successful spammers pick targets. In *Proceedings of the 28th Annual Computer Security Applications Conference* (New York, NY, USA, 2012), ACSAC '12, ACM, pp. 389–398.
17. Stringhini, G., Wang, G., Egele, M., Kruegel, C., Vigna, G., Zheng, H., and Zhao, B. Y. Follow the green: growth and dynamics in twitter follower markets. In *Proceedings of the 2013 conference on Internet measurement conference* (2013), ACM, pp. 163–176.
18. Thomas, K., Grier, C., Song, D., and Paxson, V. Suspended accounts in retrospect: An analysis of twitter spam. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (New York, NY, USA, 2011), IMC '11, ACM, pp. 243–258.
19. Twitter, Huffington Post, e. Twitter Statistics. `http://www.statisticbrain.com/twitter-statistics/`, 2014.
20. Wang, A. H. Don't follow me - spam detection in twitter. In *SECRYPT* (2010), pp. 142–151.