Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A New Design for Detecting Malware in Social Networks

K.L.Akshaya Nivasini*, J. Jayapradha AP

Computer Science & Engineering & Krishnaswamy College of Engg. & Tech.
Tamil Nadu, India

***Abstract**— Social networking grows more enormously and users use this application to meet and interact online. After the growth of social networking, hackers easily hack the information of the users. Users are more addicted to these kind of social applications like facebook, twitter and so on. Through the social networking sites many cybercriminals may happen. Cybercriminals includes theft of the user information and hack their email id, passwords, etc. In this paper, we examine to which level spam has enter social networks. In addition, we analyse spammers who target social networking sites operate. To gather the data regarding spamming activity, we developed a enormous plus dissimilar set of "honey-profiles" on three large social network sites, additionally logged the type of contacts and messages that they received. We next evaluate the collected information and recognized abnormal actions of users who contacted our profiles. Based on the investigation of this performance, we developed technique to detect spammers in social network, and we aggregate their messages in large spam campaigns. Our outcome show that it is possible to automatically recognize the accounts used by spammers, and our analysis was used for take-down efforts in a real-world social network. More exactly, during this study, we collaborated with Twitter and correctly detected and deleted 15,857 spam profiles.*

***Keywords**— Social Network, honey profiles, spamming activity, cybercriminals*

I. INTRODUCTION

Over the last few years, social network site have turn into one of the main ways for user to remain track and communicate with their associates online. Most social networks offer mobile platform that permit user to access their services from mobile phones, making the access to these sites ubiquitous. Unfortunately, this wealth of information, as well as the ease with which one can arrive at lots of user, in addition concerned the attention of malicious party. In exacting, spammers are evermore seemed designed for way to arrive at latest victims with their unsolicited messages. This is shown by a market survey about the user sensitivity of spam over social networks, which shows that, in 2008, 83% of the users of social networks have received at least one unnecessary companion request or message .From a security point of view, social networks have single characteristics. First, information access and interface is based on belief. Users typically distribute a large amount of personal information with their friends. This information may be public or not. Unfortunately, social networking sites do not offer strong verification mechanism, and it is simple to impersonate a user and sneak into a person's network of trust [15]. Additionally, it often happen that user, to gain popularity, accept any companionship request they receive, exposing their private information to strange people. As a result, anybody can access it, friend or not. Networks of belief are significant from a security point of view, because they are often the only mechanism that protect user from being contacted by unnecessary entities. While most user have become aware of the common threats that affect the Internet, such as e-mail spam and phishing, they usually do not show a sufficient appreciative of the threats hidden in social networks. For example, a previous study showed that 45% of users on a social networking site readily click on links posted by their "friend" accounts, even if they do not know that person in real life [10]. This behavior might be abused by spammers who want to advertise web sites, and might be particularly harmful to users if spam messages contain links to malicious pages. Even though social networks have raised the attention of researchers, the problem of spam is still not well understood. This paper presents the results of a year-long study of spam activity in social networks. The main contributions of this paper are the following:

- We formed a set of honey net accounts (honey-profiles) on three main social networks, and we logged all the movement (malicious or not) these account were able to examine above a one-year time for Facebook.
- We examine how spammers are using social networks, and we observe the efficiency of the counter-measures that are taken by the main social network portals to avoid spamming on their platform.
- We recognize distinctiveness to facilitate permit us to identify spammers in a social network.
- We build a device to identify spammers, and used it on a Facebook dataset**.**

II. BACKGROUND AND RELATED WORK

Social networks suggest a method for user to remain track of their friends and communicate with them. This system of belief normally regulates which private information is observable to whom. In our work, we look at the dissimilar ways in which social networks run the network of trust and the visibility of information between users. This is significant since the nature of the network of belief provide spammers with dissimilar option for transfer spam messages, knowledge information about their victims, or befriends an important person (to appear reliable and make it more tough to be detect as a spammer).

A. The Facebook Social Network

Facebook is presently the leading social network on the Internet. Regularly, user profiles are not public, and the right to sight a user's page is approved only after having recognized an association of belief (paraphrasing the Facebook terminology, becoming friends) with the user. When a user A wants to become friend with another user B, the stage first send a request to B, who has to acknowledge that she knows A. When B confirms the request, a friendship connection with A is established. However, the users' perception of Facebook friendship is different from their perception of a relationship in real life. Most of the time, Facebook users accept friendship requests from persons they barely know, while in real life, the person asking to be friend would undergo more scrutiny. The default privacy setting for Facebook was to permit all people in the identical network to view each other's profiles. Thus, a malicious user could connect a big network to move slowly data from the users on that network. This data allows an adversary to carry out targeted attacks. For example, a spammer could run a campaign that targets only those users whose profiles have certain characteristics (e.g., gender, age, interests) and who, therefore, might be more responsive to that campaign. For this reason, Facebook deprecate geographic networks in October 2009. School and company networks are still available, but their security is better, since to join one of these networks, a user has to provide a valid e-mail address from that institution (e.g., a university e-mail address).

B. Related Work

The achievement of social networks has concerned the notice of safety researcher. In 2008, a Sophos experiment showed that 41% of the Facebook users who were contact approved a friend request from a random person [8]. Bilge et al. [10] show that after an attacker has entered the network of trust of a victim, the victim will likely click on any connection enclosed in the messages posted, irrespective of whether she knows the attacker in real life or not. Another motivating verdict was reported by Jagatic et al. [13]. The author found those phishing attempts are additional probable to achieve something if the hacker uses stolen information from victims' friends in social networks to skill their phishing emails. Another work that studied social network spam using honey-profiles was conducted by Webb et al. in 2008 [17]. The study showed a important spam activity. The honey-profiles were contacted by 1,570 spam bots over a five-month period. Moreover, we leverage our surveillance to build up a system capable to detect spammers on social networks. This system has detected thousands of spam accounts on facebook, which have been consequently deleted.

III. DATA COLLECTION

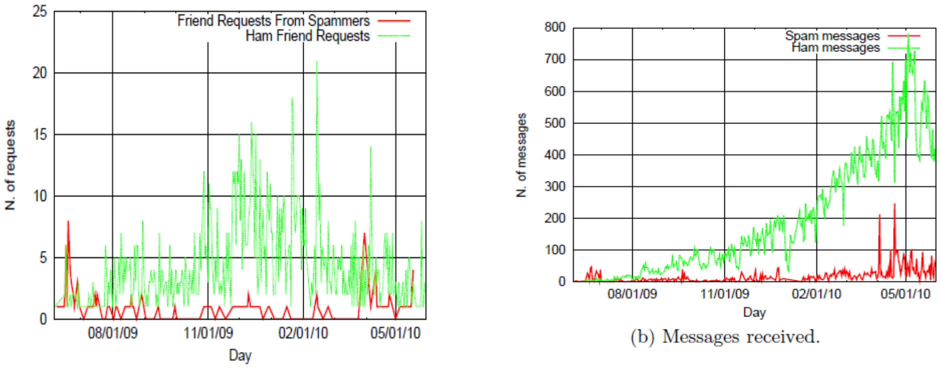
The primary aim of our manuscript was to recognize the degree to which spam is a trouble on social networks, as well as the description of spam activity. The idea of these accounts was to log the traffic (e.g., friend requests, messages, invitations) they obtain from other users of the network. Due to the correspondence of these profiles to honeypots [4], we describe these accounts honey-profiles.

A. Honey-Profiles

Our aim was to make a numeral of honey-profiles that imitate a delegate choice of the inhabitants of the social networks we analyzed. To this conclusion, we foremost crawl every social network to gather general profile information. On Facebook, we connected 16 geographic networks, by means of a little quantity of manually-created accounts. This was probable since, at the instance, geographic networks were still accessible. Since we wanted to make profiles reflecting a diverse population, we connected network on all continents (except Antarctica and Australia): the Los Angeles and New York networks for North America, the London, France, Italy, Germany, Russia, and Spain ones for Europe, the China, Japan, India, and Saudi Arabia ones for Asia, the Algeria and Nigeria ones for Africa, and the Brazil and Argentina networks for South America. For each network, we crawled (which is the basic information required to create a profile on Facebook). Afterwards, we arbitrarily varied this information (names, surnames, and ages) and formed the honey-profiles. Gender was determined by the first name. Each profile was assigned to a network. Accounts created using data from a certain network were assigned either to this network or to a network where the main language spoken was the same (e.g., profiles created from accounts in the France network were used in networks associated with francophone countries). This was a physical process. For bigger network (e.g., New York, Germany, Italy) up to three accounts were formed, while only one account was set up for smaller ones. In total, we created 300 accounts on the Facebook platform. After data collection, we looked for general names and ages from profiles with dissimilar language, and formed profiles in most nations of the world. While on Facebook birth date and gender are needed for registration whereas on Twitter, the only information required for signing up is a full name and a profile name. Therefore, we did not find it essential to move slowly the social network for "average" profile information, and we simply used first names and surnames from the other social networks. For each account, the profile name has been chosen as a concatenation of the first and last name, plus a chance number to avoid conflict with already existing accounts. More accurately, even though we could automatically fill the forms required for registration, we still required a person to solve the CAPTCHAs concerned in the method.

B. Collection of data

After having formed our honey-profiles, we ran scripts that every so often linked to those accounts and checked for activity. We determined with the intention of our accounts should act in a passive way. As a result, we did not send any friend requests, but established all those that were acknowledged. In a social network, the primary accomplishment a malicious user would likely implement to get in touch with his victims is to send them a friend request. This capacity be complete to catch the attention of the user to the spammer's profile to sight the spam messages or to invite her to agree to the friendship and start considering the spammer's messages in her own feed (on Facebook). After having approved a request (i.e., accepted the friendship on Facebook), we logged all the information wanted to notice malicious activity. More accurately, we logged each email announcement acknowledged from the social networks, as well as all the requests and messages seen on the honey-profiles. On some networks, such as Facebook, the notification and messages might be of dissimilar type (e.g., application and group invitations, video posts, status messages, private messages), while on other platforms, they are more uniform (e.g., on Twitter, they are always short text messages). We logged all type of requests on Facebook, as well as wall posts, status updates, and private messages. Our scripts ran continuously for 12 months for Facebook (from June 6, 2009 to June 6, 2010). The visits have to be perform gradually (approximately one account visited every 2 minutes) to stay away from being detect as a bot by the social networking site and, consequently, have the account delete.



(a) Friend requests received.

(b) Messages received.

Figure 1: Activity observed on Facebook

IV. ANALYSIS OF COLLECTED DATA

As mentioned before, the primary act that a spammer would possible perform is to send friend requests to her victims. Merely a portion of the contact user will recognize a request, since they do not be familiar with the real-life person linked with the account used by the bot1. On social network, the idea of companionship is somewhat dissimilar, but the modus operandi of the spammers is the same: they begin next victims, hoping that they will follow them back, starting to receive the spam content. From the viewpoint of our examination, friendships and shared follow relationships are the same. When users accept one of the friend requests, she lets the spammer go into her network of trust. In practice, this action has a major consequence: The victim starts to see messages received from the spammer in her own news/message feed. This kind of spamming is very efficient, because the spammer has only to write a single message (e.g., a status update on Facebook), and the message appear in the feed of everyone victims. Daily statistics for friend requests received on Facebook are shown in Figures 1(a). Information about the logged messages is shown in Table 2. Overall, we observed 85,569 messages. Again, there is a big difference sandwiched between the three social networks Daily information for messages received on Facebook are shown in Figure 1(b), while those for Twitter are reported in Figure 2(b). On Facebook, we also observed a fair total of invitation to applications, groups, and events, as well as posting of photos and videos in our honey-profiles' feeds. Yet, since none of them were spam, we ignored them for the succeeding investigation.

Network	Overall	Spammers
Facebook	3,831	173
MySpace	22	8
Twitter	397	361

Table 1: Friend requests received on the various social networks.

Network	Overall	Spammers
Facebook	72,431	3,882
MySpace	25	0
Twitter	13,113	11,338

Table 2: Messages received on the various social networks.

A. Identification of spam accounts

During this method, we notice that spam bots share some frequent traits, and dignified them in features that we then used for automated spam detection. We will describe these features in detail in Section 5. We found that, of the original

3,831 accounts that contacted us on Facebook, 173 were spammers. Moreover, on Facebook, during the last months of logging, the ratio of spam messages compare to genuine ones noticeably dropped. The cause is that when a justifiable user adds our honey-profile to her friend list, this honey-profile starts appearing on her friends' pages as a friend suggestion.

B. Spam bot analysis

The spam bots that we recognized show dissimilar level of action and dissimilar strategy to bring spam. Based on their spam strategy, we distinguish four categories of bots:

1. Displayer: Bots that do not post spam messages, but only exhibit some spam content on their own profile pages. This kind of bots is likely to be the least efficient in conditions of people reached.

2. Bragger: Bots that post messages to their own feed. These messages differ according to the networks.

3. Poster: Bots that send a straight message to every victim. This can be achieving in dissimilar behaviour, depending on the social network. On Facebook, for example, the message might be a post on a victim's wall. The spam is shown on the victims feed, but, distinct the case of a "bragger", can be viewed also by victim's friends visit her profile page.

4. Whisperer: Bots that send private messages to their victims. As for "poster" bots, these messages have to be address to a definite user. The distinction, however, is that this time the victim is the only one considering the spam message. This type of bots is fairly common on Twitter, where spam bots send direct messages to their victim. We observed 20 bots of this kind on this network, but nothing on Facebook.

V. DATA COLLECTION

Based on our sympathetic of spam action in social networks, the subsequently objective was to influence these insights to build up technique to notice spammers in the wild. We determined to focus on detecting "bragger" and "poster" spammers, since they do not need real profile for recognition, but are just noticeable by look at their feeds. We used machine learning techniques to categorize spammers and legal users.

A. Spam detection on Facebook

The major subject when analyze Facebook is to get a appropriate quantity of information to examine. Most profiles are personal, and merely their friends can perceive their walls. At the start of this learn, geographic networks were still obtainable, except they were discontinue in October 2009. Consequently, we used information from various geographic networks, crawl between April 28 and July 8 2009, to test our approach. Since on Facebook the number of friend requests sent out is not open, we could not apply the R feature. We train our classifier using 1,000 profiles. We used the 173 spam bots that contact our honey-profiles as samples for spammers, and 827 manually checked profiles from the Los Angeles network as samples for legitimate users. A 10-fold cross validation on this training data set yielded an estimated false positive ratio of 2% and a false negative ratio of 1%. We then apply our classifier to 790,951 profiles, belong to the Los Angeles and New York networks. We detect 130 spammers in this dataset. Among these, 7 were false positives. The motive for this low number of detect spammers might be that spam bots typically do not join geographic networks. This theory is corroborated by the fact that among the spam profiles that contacted out honey profiles, none was a member of a geographic network. We then arbitrarily chosen 100 profiles, classified as legal. We physically looked at them to search for false negatives. None of them twisted out to be a spammer.

B. Identification of spam campaigns

After having recognized particular spammers, we analyze the information to recognize larger scale spam campaigns. With "spam campaign," we refer to several spam profiles that act beneath the organization of a single spammer. We regard as two bots posting messages with URLs pointing to the same location as being part of the equal campaign. Most bots hide the real URL that their relations are pointing to by means of URL restriction services (for example, tinyurl [6]). This is typically done to keep away from easy finding by social networks administrator and by the users, as well as to gather the message length necessities of some platforms. To launch the real site that a reduced URL points to, we visited all the URLs that we experimental. After that, we clustered all the profile that advertises the same page. We catalog the top eight campaigns, based on the number of experiential messages, in Table 3. It is motivating to notice, however, that bots belong to three of them were practical on facebook as well.

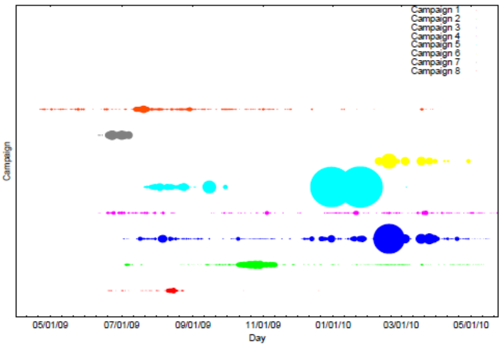


Figure 3: Activity of campaigns over time.

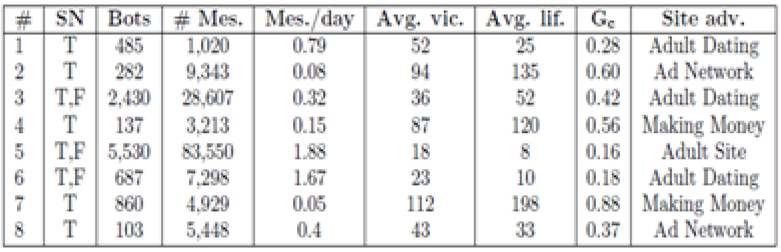
From the explanation of a variety of campaigns, we developed a metric that allows us to forecast the achievement of a campaign. We regard as a campaign successful if the bots belong to it have a long life span. For this metric, we initiate the limit Gc, defined as follows:

$$G_c = \frac{M_d^{-1} \cdot S_d}{((\sqrt{M_d^{-1} \cdot S_d})+1)^2},\ 0 \leq G_c \leq 1.$$

In the exceeding method, Md is the average number of messages per day sent and Sd is the ratio of actual spam messages (0 _Sd _ 1). Empirically, we observe that campaign with a value of Gc close to 1 have a long life span (for example, Campaign 7 has Gc = 0.88, while Campaign 2 has Gc = 0.60), while for campaigns with a lower value of this limit, the regular lifetime decrease considerably (Campaign 1 has Gc = 0.28 and Campaign 5 has Gc = 0.16). Thus, we can infer that a value of 0.5 or higher for GC indicates that a campaign has a good chance to be successful. Of course, if a campaign is lively for some time, a social network might build up other means to notice spam bots belong to it (e.g., a blacklist of the URLs included in the messages).

Activity of bots from dissimilar campaign is shown in Figure 3. Each row represents a campaign. For each day in which we experimental some action from that campaign, a circle is drawn. The dimension of circles varies according to the number of messages observed that day. As can be seen, some campaigns have been lively over the whole period of the study, while some have not been so flourishing.

Table 3: Spam campaigns observed.



#	SN	Bots	# Mes.	Mes./day	Avg. vic.	Avg. lif.	G_c	Site adv.
1	T	485	1,020	0.79	52	25	0.28	Adult Dating
2	T	282	9,343	0.08	94	135	0.60	Ad Network
3	T,F	2,430	28,607	0.32	36	52	0.42	Adult Dating
4	T	137	3,213	0.15	87	120	0.56	Making Money
5	T,F	5,530	83,550	1.88	18	8	0.16	Adult Site
6	T,F	687	7,298	1.67	23	10	0.18	Adult Dating
7	T	860	4,929	0.05	112	198	0.88	Making Money
8	T	103	5,448	0.4	43	33	0.37	Ad Network

We next try to recognize how bots prefer their victims. The performance seems not to be regular for the various campaigns. For example, we notice that many victims of Campaign 2 shared the same hashtag (e.g., "#iloveitwhen") in their tweet. Bots might have been crawling for people sending messages with such tag, and started following them. On the other hand, we notice that Campaigns 4 and 5 embattled an abnormal number of private profiles. Looking at their victims, 12% of them had a private profile, while for a random picked set of 1,000 users from the public timeline, this ratio was 4%. This suggests that bots from this campaign did not move slowly any timeline, since tweets from users with a personal profile do not emerge on them.

VI. CONCLUSIONS

Social networking sites have millions of users from all over the world. The easiness of accomplishment these users, as well as the option to take benefit of the information stored in their profiles attracts spammers and other malicious users. In this paper, we showed that spam on social networks is a problem. For our study, we formed a population of 900 honey-profiles on three major social networks and experimental the traffic they received. We then developed techniques to distinguish single spam bots, as well as large-scale campaigns. We also showed how our techniques help to sense spam profiles even when they do not contact a honey-profile. We believe that these techniques can help social networks to growth their security and notice malicious users. In fact, we build up a device to detect spammers on Twitter. Providing Twitter the results of our analysis thousands of spamming accounts were shut up down.

ACKNOWLEDGMENT

This work was supported by the ONR under grant N000140911042 and by the National Science Foundation (NSF) under grants CNS-0845559 and CNS-0905537.

REFERENCES

[1] Alexa top 500 global sites. http://www.alexa.com/topsites.

[2] Compete site comparison. http://siteanalytics.compete.com/facebook.com+myspace.com+twitter.com/.

[3] Facebook statistics. Http://www.facebook.com/press/info.php?statistics.

[4] Honeypots. Http://en.wikipedia.org/wiki/Honeypot_computing.

[5] The recaptcha project. http://recaptcha.net/.

[6] Tinyurl. http://tinyurl.com/.

[7] Weka - data mining open source program. http://www.cs.waikato.ac.nz/ml/weka/.

[8] Sophos facebook id probe. http://www.sophos.com/pressoffice/news/ articles/2007/08/facebook.html, 2008.

[9] J. Baltazar, J. Costoya, and R. Flores. Koobface: The largest web 2.0 botnet explained. 2009.

[10] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In World Wide Web Conference, 2009.

[11] L. Breiman. Random forests. In Machine Learning, 2001.

[12] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam.In ACM Conference on Supportive Cooperative Work,2008.

[13] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and T.N.Jagatif. Social phishing. Comm. ACM, 50(10):94–100, 2007.

[14] B. Krishnamurthy, P. Gill, , and M. Aritt. A few chirps about twitter. In USENIX Workshop on Online Social Networks, 2008.

[15] S. Moyer and N. Hamiel. Satan is on my friends list: Attacking social networks. http://www.blackhat.com/html/bh-usa-08/bh-usa-08-archive.html, 2008.

[16] Harris Interactive Public Relations Research. A study of social networks scams. 2008.

[17] S. Webb, J. Caverlee, , and C.Pu. Social honeypots: Making friends with a spammer near you. In Conference on Email and Anti-Spam (CEAS 2008),2008.

[18] S. Yardi, D. Romero, G. Schoenebeck, and D. Boyd. Detecting spam in a twitter network. First Monday,15(1), 2010.