Impact of fake profiles on social medias

pierre-louis.gottfrois@epitech.eu
pierre.fourgeaud@epitech.eu
sacha.ott@epitech.eu

March 22, 2012

Abstract

Social media websites such as Facebook or Twitter have become increasingly popular as a way to meet and converse with friends, co-workers and even people you don't know. At the same time, security concerns inherent in such communication have been explored in various different ways. Also fake profiles is a serious security threat to human communication in social media.

This paper presents the concern about social media bots and their goals in today's context. The paper further describes countermeasures in order to identify such threats.

1 Introduction

Online Social Networks (OSNs) such as Facebook and Twitter have successfully accomplished their goal of connecting people together. With millions of active users using their platforms every day, they have reach a point where third party companies want to exploit them as an effective media to reach and potentially influence a large and diverse population of web users. For example, there are now more than 850 million active Facebook users, with more than 200 million added in 2011 and over 140 million active Twitter users [3].

It is now common for web users to share their personal and professional lives using OSNs. Today's users use Internet, cell phones and mobile devices every day to talk, socialize and share "things" with their family, friends and colleagues. However, online social experience is not exclusive to only human beings.

A new kind of computer programs called "socialbots" are now online, gathering huge amount of informations and trying to socialize with real users in order to potentially influence them. A socialbot is an automation software who will automatically take control of an online account on a particular OSN. It has the ability to do basic actions such as posting contents and sending connection requests to real users. Most advanced socialbots are made in a fashion way such as they can interact with real users without being spotted. This allows the socialbot to "infiltrate" user's connections in order to reach an influential position, that is, to spread misinformation and propaganda in order to bias the public opinion, perform surveillance, and even more.

In this paper, we recovered data analytics from various sources that show today's statistics on OSNs. We presented different ways of how to recognize a socialbot on Facebook in order to identify what are the recurrent patterns seen in fake profiles. From the user side, we show that a lot of OSN users are not careful enough when dealing with connection requests. Even more when they share mutual connections with the sender. This is one behavior being exploited by socialbot makers to achieve a large-scale infiltration with a high success rate. Finally, we presented first some basic techniques used by socialbot makers in comparison of more advanced techniques used to have more accurate socialbots capable of almost pass themselves as human beings.

In conclusion, we discussed the importance of the human factor in such threats and how OSN designers are trying to deal with them.

2 Preliminaries

2.1 Online Social Networks

An Online Social Network (OSN) is an online service, platform or site that focuses on building and reflecting of social networks or social relations among people, who, for example, share interests and/or activities. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services [5].

2.2 Socialbots

A socialbot is an automation software who will automatically take control of an online account on a particular OSN. It has the ability to do basic actions such as posting contents and sending connection requests to real users. More advance socialbot are using heuristics and learned observations about user's behavior in order to increase the magnitude of their potential damage. Socialbot's main goal is to imitate real user's behavior as close as possible and to perform scalable attacks in a particular OSN.

3 Online Social Networks Statistics

3.1 Facebook

Facebook is a social networking service and website launched in February 2004. After 8 years, Facebook has more than 845 million active users. A January 2009 study ranked Facebook as the most used social networking service by worldwide monthly active users [4].

With 50.3% of North America population, 57% users on facebook said to talk to people more online than they do in real life. 48% of young Americans said they find out about news through facebook [1].

It is obvious that Facebook is a good place for socialbot makers. The huge number of users using facebook every day makes this OSN the place with the maximum likelihood to trap real users with fake accounts.

3.2 Twitter

Twitter is an online social networking service and micro-blogging service that enables its users to send and read text-based posts of up to 140 characters, known as "tweets". It was created in March 2006 and launched that July. The service rapidly gained worldwide popularity, with over 465 million users as of 2012, generating over 175 million tweet per day [6].

It has been described as "the SMS of the Internet." Both private Internet users and public corporations have embraced the micro-blogging site to share news, photos, links and more.

Once again socialbot makers are looking after Twitter's functionalities. As a matter of fact, interesting content will be re-tweet by users within 92% compare to 84% due to personal connections. We can see here that not only because the content might be interesting but also because users usually trust their social network and their friends. This is a crucial fact for socialbot makers to know as their goal is to act at large-scale.

4 How to recognize a Socialbot ?

In this section we extracted statistics from various sources showing what are the ways to recognize fake profiles over real profiles on Facebook. As a matter of fact, we found that 97% of fake profiles are female. Moreover, 58% of them are interested in both men and women against only 6% for real people. Profile picture is also a good clue with almost always a picture of an attractive women.

We also found that a majority of fake profiles do not update their social status. In fact 43% of them have never updated their Facebook status compared to 15% of real people. Even more interesting, on average, fake profiles' pictures have 136 "tags" every 4 pictures against an average of 1 "tag" for real users. People interests also have big differences, the average number of entertainment interests listed is 3 for fake profiles against 12 for real profiles. Moreover, 68% of fake profiles claim to have attended college over 40% for real users.

Finally, the easiest way to detect fake profile is with the number of social connections (friends). In deed, the average number is 130 friends for real people against 726 friends for fake profiles. We can see here that there is a very large disparity between fake and real profiles on Facebook. However it may not be so obvious for people not aware on how to recognize fake profiles from real ones.[2]

5 Socialbot makers techniques

5.1 Objectives

There are two main objectives when creating a socialbot: (1) to carry out a large-scale infiltration campaign in the targeted OSN, and (2) to harvest private user's data. In order to achieve these goals, the socialbot need to connect to a large number of either random or targeted OSN users.

Whereas collecting user's data create great opportunities for socialbot makers to do some phishing, spam or even collect monetary valuable data.

5.2 Construction

In this part, we will not cover the network architecture needed to handle large-scale socialbots. It is absolutely necessary that such network provide some way to minimize traffic to avoid detection.

Building a socialbot involves first creating an attractive profile in the targeted OSN. After that the credentials are given to the socialbot in order to get full control over this profile.

Second, research shows that the social attractiveness of a profile in an OSN is highly correlated to its neighborhood size. For example, 130 connections is the average on Facebook. Thus, in order to increase the social attractiveness of a socialbot, the adversary orders each socialbot to connect to at most N_{avg} other socialbots.

Third, it is well known that when two users share mutual connections, they are more likely to connect to each other. Therefor in order to improve the potential infiltration in the targeted OSN, the adversary orders each socialbot to connect to user profiles with whom it has mutual connections.

Finally, whenever a socialbot is connected to a user profile, the adversary orders the socialbot to collects all accessible user's profile information in its neighborhood.

In order to be effective, a socialbot has to meet two challenging goals: (1) socialbots need to be well developed in order to hide themselves from OSN, and (2) to implement heuristic that enable large-scale infiltration on targeted OSN.[7]

6 Conclusion

We have discussed what are the existing threats on OSN and saw various techniques on how to recognize socialbots. We talked specially about Facebook because we believe it is the biggest and more popular OSN right now with its millions of users. We saw what needed to be done in theory to create a socialbot to take over at large scale on a targeted OSN. Unfortunately it is obvious that socialbot makers are already taking advantages of these opportunities at large scale in order to make money and/or to influence people in real world. We believe that such infiltration in OSNs is only one over multiple future threats agains social networks and defending agains such threats is the first step towards maintaining a safer social Web for all of us.

7 Acknowledgments

We would like to thank you all people for their feedback on an early draft of this paper.

References

[1] CompetePulse. Social networks: Facebook takes over top spot, twitter climbs, 2009. http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/.

[2] Barracuda Labs. Facebook user profiles. http://www.barracudalabs.com/fbinfographic/.

[3] Mediabistro. Stats of the day, 2012. http://www.digitalbuzzblog.com/social-media-statistics-stats-2012-infographic/.

[4] Wikipedia. Facebook, March 2012. http://en.wikipedia.org/wiki/Facebook.

[5] Wikipedia. Social networking service, 2012. http://en.wikipedia.org/wiki/Social_networking_service.

[6] Wikipedia. Twitter, March 2012. http://en.wikipedia.org/wiki/Twitter.

[7] Konstantin Beznosov Matei Ripeanu Yazan Boshmaf, Ildar Muslukhov. The socialbot network: When bots socialize for fame and money. page 4, February 2012.