Socialbot & Online Social Networks

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

March 15, 2012

Abstract

Social media website 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 rich a point where third parties companies wants 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 800 million active Facebook users, with more than 200 million added in 2011 and over 100 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 data 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 connections requests to real users. Most advance socialbot 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 shows 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 advance 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 connections 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 account.

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 connection. 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 ?

97% of fake profiles are female. Moreover, 58% of them are interested of both men and women. With this information, we can be suspicious about this profile. But the main thing about fake profile is the photo. Often, a fake profile will have a pretty attractive women attached to it.

Another thing is that the majority of fake profiles didn't update their status on the social media platform. Fake profiles have also an average of 136 tags every 4 photos on their profile against an average of 1 for real users. Besides, interest information is about (3) against (14) for a real profile. Like the education, who is about () in average against () for normal user.

Another big issue with fake users, is that they have an average of 726 friends against an average of 130. Mainly, fake users have fake links in their profile with many ads. A big fact, is that their is no delay between answer from a fake user, like when you type something, instantly the fake profile answer because it's a program (we call that kind of program, a bot). [2]

5 Socialbot makers techniques

6 Conclusion

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.