# [POSTER] The Socialbot Network: When Bots Socialize for Fame & Money

Yazan Boshmaf[*], Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu
University of British Columbia, Vancouver, Canada

## 1 Introduction

A new breed of computer programs called socialbots are now online, and they can be used to breach users' privacy, spread misinformation to bias the public opinion, and compromise the graph of a targeted social network [1, 2]. A socialbot controls a fictitious user profile and has the ability to execute basic online activities (e.g., posting a message, sending a connection request). What makes a socialbot different from other self-declared bots (e.g., bots posting weather forecasts in Twitter) is that it is designed to infiltrate online communities by passing itself off as a human being.

Socialbots can be used to manipulate the graph of a targeted social network in order to establish a centralized or influential social position in it. This position can be then exploited to mount DDoS attacks, promote products, or to spread propaganda in a viral way. For example, Ratkiewicz et al. [2] described the use of Twitter bots to spread misinformation in the run-up to the US political elections.

As the socialbots infiltrate a targeted social network, they also harvest valuable users' data which is useful for online profiling and large-scale spam campaigns. In fact, a new report showed that spammers are turning to online social networking platforms for distributing their messages [7], which explains the dramatic drop in the world-wide email spam during the recent months [6]. This gave rise to black-market businesses that offer multi-featured socialbots for as high as $29 per bot [3].

Many techniques have been proposed that try to identify socialbots based on their likely unordinary behavior (see [4] for an example on Twitter). In this research, we take a proactive step and investigate the feasibility of operating an *organized* army of socialbots which we call a Socialbot Network (SbN). A SbN is a group of socialbots that collaborate in infiltrating social networks under the orchestration of one or many "master" bots. We study the security and privacy implications of operating such a SbN on a large scale. In particular, we answer questions about the types of collaboration these socialbots can utilize, the required infrastructure, the network-wide observations that can be exploited to improve the potential infiltration, and the economics of operating a SbN on a large scale. Finally, we present a set of challenges that future social network security systems have to overcome in order to mitigate the potential threat of a SbN.

## 2 Our Approach

We decided to adopt a botnet-like infrastructure for operating a SbN as (1) it provides the required scalability to manage a large number of socialbots, and (2) it is expected that an attacker operates a SbN on top of an existing botnet, along with other malicious software. Accordingly, we define a SbN as a set of socialbots that are owned and maintained by a human controller called the bot-herder. In particular, a SbN consists of three essential components: socialbots, a bot-master, and a C&C channel. Each socialbot has to be able to execute social-interaction related commands (e.g., post a message) and social-structure related commands (e.g., send a connection request), all of which are either sent by the bot-master or predefined locally in each socialbot. All data collected by the socialbots is called the bot-cargo and is sent back to the bot-master. A bot-master (a.k.a. C&C server) is an automation software that the bot-herder interacts with in order to send commands through the C&C channel. Moreover, the bot-master builds new socialbots and implements the logic that exploits network-wide heuristics and observations about users' behavior in the targeted social network. The C&C channel is a communication channel that facilitates the transfer of both the bot-cargo and the commands between the socialbots and the bot-master. Figure 1 shows a conceptual model of a SbN.

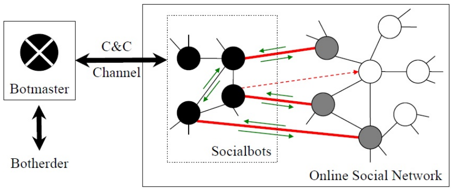

Figure 1: A conceptual model of a SbN in a toy social network. Each node represents a user profile in the network. Edges between nodes represent social connections. The socialbots are marked in black. The dashed arrow represents a connection request (a social-structure operation), and the small arrows represent read/write information flow (social-interaction operations).

We built a semi-automated SbN that operates on Facebook. We chose Facebook as a targeted social network because it is particularly difficult to operate a SbN on it for the following reasons: (1) Facebook is mostly used to connect to offline (i.e., real-life) friends and family [8], and (2) Facebook employs the Facebook Immune System [5].

Our preliminary results show that: (1) The more friends a user has on Facebook, the higher the chance that the user accepts a friendship request from a socialbot. (2) This chance improves if the socialbot establishes mutual friends with that user. (3) Most of the socialbots have relatively similar infiltration size (i.e., number of friends). (4) Most of Facebook users decide to accept a friendship request within a period of three days. (5) The socialbots harvest orders of magnitude more users' profile information (e.g., email addresses, phone numbers, birth dates) compared to public access.

**Acknowledgments:** This research is sponsored by a grant from NSERC Internetworked Systems Security Network (ISSNet).

## References

[1] Realboy: Believable Twitter bots. `http://ca.olin.edu/2008/realboy` (last accessed July 11, 2011).

[2] J. Ratkiewicz et al., "Truthy: Mapping the spread of astroturf in microblog streams," in WWW'11, 2011.

[3] Jet bots. `http://allbots.info` (last accessed July 11, 2011).

[4] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in ACSAC'10, 2010.

[5] T. Stein, E. Chen, and K. Mangla, "Facebook immune system," in SNS'11, 2011.

[6] G. Morgan, " Global spam e-mail levels suddenly fall," `http://www.bbc.co.uk/news/technology-12126880` (last accessed July 11, 2011).

[7] S. Patil. "Social network attacks surge," `http://www.symantec.com/connect/blogs/social-network-attacks-surge` (last accessed July 11, 2011).

[8] N. Ellison, C. Steinfield, and C. Lampe, "The benefits of Facebook Friends: Social capital and college students' use of online social network sites," Computer-mediated Communication, 2007.

[*] Corresponding author. Email: boshmaf@ece.ubc.ca