The SocialBot Network
When Bots Socialize for Fame and Money

Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu
**IPO : Facebook par les chiffres**

<table>
<thead>
<tr>
<th>IPO (Initial Public Offering)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Levée de fonds</strong></td>
</tr>
<tr>
<td>Valorisation estimée</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Utilisateurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilisateurs actifs / mois</td>
</tr>
<tr>
<td>Utilisateurs mobiles / mois</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Résultats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chiffre d'affaires en 2011</td>
</tr>
<tr>
<td>Bénéfice net en 2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Répartition des revenus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publicité</td>
</tr>
<tr>
<td>% sur la vente d'applications</td>
</tr>
<tr>
<td>Dont 445,3 millions $ issus de Zynga (12%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mark Zuckerberg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rémunération annuelle</td>
</tr>
<tr>
<td>Capital détenu</td>
</tr>
<tr>
<td>Droits de vote détenu</td>
</tr>
</tbody>
</table>
Reaching Out to Millions

Obama Raised Half a Billion Online in 2008

(source: Jose Vargas, Voices on The Washington Post, November, 2008)
Mobilizing the Masses

The Arab Spring, January 2011 - Now

Photo credit: Peter Macdiarmid, Getty Images

Photo credit: Steve Crisp, Reuters
Predicting the Future: UK General Election 2010


Predicting the Future: Markets

Twitter mood (*Calm*) predicts Dow Jones Industrial Average (*DJIA*)

Day-to-day Overlap

*Calm* lagged by 3 days

Bots and SocialBots

'bot‘ - computer program used to perform highly repetitive operations,
(source: UrbanDictionary.com)

Automation Software (to pass as human) + Social media account { SocialBot
Rise of the SocialBots

Zack Coburn and Greg Marra, Olin College, 2010

The Web Ecology Project (Social Engineering), 2011

ACM Interactions Magazine, Cover Story
April, 2012
Misusing SocialBots on a Large Scale?

A scalable approach for

Infiltration  Misinformation  Data collection
Project Goals

• Evaluate the feasibility of large-scale infiltration by a group of orchestrated socialbots

• Characterize users’ behavior in response to such infiltration

• Investigate the corresponding privacy and security implications

• Improve security mechanisms
Botmaster

C&C Channel

BotHerder

SocialBots

Infiltrated user (randomly picked)

Infiltrated user (with mutual friends)

Online Social Network

Concept

SocialBot
Evaluation
Methodology

• Prototype on Facebook
• 102 SocialBots, single BotMaster
• Operated for 8 weeks
• Single machine
  • Different IPs
  • HTTP proxy emulating different browsers and OSs
• Approved by UBC ethics board
Prototype Architecture

- BotUpdater
- Master Controller
- C&C Engine
- Botmaster
- API Wrapper
- HTTP Scraper
- Native Controller
- Socialbot
- 3rd Party Websites & APIs
- Blurbs, Tokens
- Access Tokens
- Our Machine
- Facebook Servers
- HTTP
- Graph API + HTTP

Updates

Commands, Botcargo

http://example.com
Infiltrated user (randomly picked)
Infiltrated user (with mutual friends)
Contacted user
Most Users Decide Within Three Days

86% of accepted requests are decided within 3 days.

58% of accepted requests are decided within 1 day.
Too Many Friends: Too Many Bots?

**f-socialbots**

Acceptance rate (%) vs. Number of friends

- 95% confidence intervals

**m-socialbots**

Acceptance rate (%) vs. Number of friends

- 95% confidence intervals

- UBC logo

23
The End Result (15 Socialbots)

8,570 request sent ➞ 3,055 accepted

20% Blocked
Mutual Friends Matter

Acceptance rate (%)

Number of mutual friends

Bootstrapping

95% conf.
Successful Infiltration is Team Work

- 88 bots infiltrated 10-40 profiles
- 10 bots infiltrated 60-80 profiles

- 70% success rate for 10-40 profiles
- 23% success rate for 60-80 profiles
Implications
Private Data Exposed

SocialBots: 102
Their friends: 3055
Friends of friends: 1,085,785

Birth dates: 48,810 before → 580,649 after (11.9x more)
Capability of “Social Adversaries”

-Sybil detection via social networks
-Attack edges
-Sybil region
-Honest region
-With adversary running large-scale infiltration
Eroding the Trust in the Web

Facebook Applications

Facebook Connect
Summary and Roadmap

- Large-scale infiltration is feasible ...
- ... and has serious privacy and security implications

- Socialbots make it difficult for OSN security defenses and their users to detect their true nature
One Socialbot’s Profile
... and furthermore ... I don't like your trousers.

Shevonna said something about Li!
Some questions your friends might have answered
1: Do you think Li is cute?
2: Would you trust Li with your life?
3: Is Li fun to be around?

This is really insane.. you have to see this

OMG.. Look What THIS Kid Did to His School After Being Expelled! WARNING: Graphic Content!
Today's average household in the USA contains more computer power than existed in the world before 1965.

I posted this before but man, this is a must-see!!

YouTube – The Coolest YouTube Rewind 2010: Year in Review
The funniest, coolest, and sickest Youtube videos in 2010. Check this out! See w...
See More

Li and Yolly Cajilig Gambaloza are now friends. · Like · Comment
Messages Received

37
Hi im from india n n anna's fren so im sending you a fren request n b fren wit u:).
hi
kimberly i feel fabulous only if u can my girly friend

babe
always thinking about u and hoping to see u one day
hi
The message is sent from Japan.
Right or wrong Please make friends with me.
August 11

Dear Laura Roy,

In a brief introduction I am Barrister Gordon King, Attorney to Late Engineer D E. Roy, a contractor and a business man who died in a motor accident along with his family.

Kindly Contact me via my private email (barrgordonking@live.com) for more information about the claim of his fund valued $13,580,000.00 United State Dollars which he deposited with the here in my country Lome-Togo.

Your urgent response will be highly appreciated.
Posts by the Socialbots
I just forgot my whole philosophy of life!!!

Like · Comment · Share · February 18 at 1:44am via Desktop Connector

likes this.

Write a comment...
No matter how much you do you never do enough.
Stay away from hurricanes for a while.

Like · Comment · Share · January 29 at 9:05am via Desktop Connector

It's good we don't have hurricanes in Kenya, we don't have capacity to deal with the aftermaths.

January 29 at 10:43am · Like

Write a comment...
Posts from Socialbots’ Friends
hy girl are you very beatiful i like your hair i want see you one day

Like · Comment · January 14 at 11:11am

Write a comment...
is your birthday?? anyway you are so pretty!

Like · Comment · See Friendship · February 12 at 9:30am

RECENT ACTIVITY

now friends with and 4 other people.
Hey Sara. Time to update your status. What is new?

Like · Comment · See Friendship · August 30 at 7:15pm
Successfully confirmed, thnks 4 da add.

Like · Comment · See Friendship · March 21 at 11:57pm
Hapi bday dear, hope you made da best out of dis day neh! *lovely-winkie*

Like · Comment · See Friendship · March 20 at 10:00am
Why did we beat Facebook’s “Immune System”?

(and why this will be a recurrent problem)
OSN Security: Adversarial Machine Learning

Stein et al., The Facebook Immune System, EuroSys – SNS, 2011
Facebook’s “Immune System” Assumptions

Fake Accounts

• Created by both scripts and raw labor
  – overcome rate limits
  – boost the reputation or ranking
  – Short lifetime

• Fake accounts have limited virality because they are not central nodes and lack trusted connections
  – Comments and wall posts on pages

Stein et al., The Facebook Immune System, EuroSys – SNS, 2011
OSN Vulnerabilities: Ineffective CAPTCHAs

CAPTCHA-solving businesses*

* Dancho Danchev, Inside India’s CAPTCHA solving business, 2008
OSN Vulnerabilities: Fake User Accounts and Profiles

“On the Internet, nobody knows you’re a dog.”
OSN Vulnerabilities: Large-Scale Network Crawls
OSN Vulnerabilities: Exploitable Platforms and APIs
What did I learn?
Facebook easily infiltrated, mined for personal info

Socialbot network could mine 175 chunks of personal data per bot per day

Robots can easily pass as real users on Facebook, allowing them to befrend real humans and mine personal information such as birthdays, addresses and phone numbers, Canadian researchers have found.

Stay Connected with CBC News

Audio
Jesse Hirsh - Socialbots 6:47

The Register

Army of 'socialbots' steal gigabytes of Facebook user data
Social networks prone to large-scale infiltration

Socialbots used by researchers to 'steal' Facebook data

Researchers have demonstrated a new technique capable of stealing personal information from Facebook.

Using 'socialbots': computer programs that mimic real Facebook profiles, the researchers were able to harvest vast quantities of personal data.

Socialbots are increasingly being used by internet criminals and are being offered for sale on the internet for as little as $29 (£18).
We are reluctant to take legal action against UBC, its researchers or students engaged in legitimate academic projects. However, this is not the first time UBC has ignored Facebook’s terms and the law. Facebook must insist that UBC and its researchers abide by Facebook’s terms and the law. Additionally, given the apparent ongoing and knowing disregard of Facebook’s terms, the law and UBC ethical obligations, we request that your offices: (1) ensure that UBC researchers cease and desist any and all unauthorized access to Facebook’s site and systems; (2) return to Facebook all illegally harvested user data obtained by UBC researchers and certify destruction of all copies that remain in UBC’s possession; (3) provide an accounting of all research activities involving Facebook and its users; (4) suspend any ongoing Facebook-related research unless and until Facebook provides consent; (5) explain the process by which UBC approved this particular study; and (6) preserve all materials that refer or relate to the UBC’s approval, or lack thereof, for studies involving Facebook and/or its users.

Again, Facebook strongly supports education and research especially in the computer and data sciences. We have no desire to chill legitimate research conducted consistent with ethical standards and the law. Once this matter is resolved, I will be happy to facilitate introductions.
Summary

• Large-scale infiltration is feasible and has serious privacy and security implications

• Effective, socio-technical defenses less vulnerable to both human and technical exploits are needed
The Socialbot Network
When Bots Socialize for Fame and Money

Yazan Boshmaf
Ildar Muslukhov
Konstantin Beznosov
Matei Ripeanu

Funded by:
Fake Accounts

• Created by both scripts and raw labor
  – overcome rate limits
  – boost the reputation or ranking
  – Short lifetime

• Fake accounts have limited virality because they are not central nodes and lack trust
  – Comments and wall posts on pages
Web-based Botnet Integration

Infected Machines

C&C Channel

Botmaster

Botherder

Botnet + Socialbot Network

OSN Channel

Socialbots

Online Social Network
Operations & Commands

Table 1: The generic operations supported by a socialbot in any given OSN.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read( o, p)</td>
<td>Social-interaction</td>
<td>Reads an object o from profile p and returns its value v as botcargo</td>
</tr>
<tr>
<td>write( v, o, p)</td>
<td>Social-interaction</td>
<td>Writes value v to object o on profile p</td>
</tr>
<tr>
<td>connect( b, p)</td>
<td>Social-structure</td>
<td>Sends or accepts a connection request sent from profile b to profile p</td>
</tr>
<tr>
<td>disconnect( b, p)</td>
<td>Social-structure</td>
<td>Breaks the social connection between profiles b and p</td>
</tr>
</tbody>
</table>

Table 2: Master commands. The socialbot b ∈ B is the socialbot executing the command, |B| = n.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Connects b to at most N_avg other socialbots in B</td>
</tr>
<tr>
<td>rand_connect( k)</td>
<td>Connects b to k non-botherder-owned profiles that are picked at random from the OSN</td>
</tr>
<tr>
<td>decluster</td>
<td>Disconnects b from every socialbot b ′ 2 S where S = {b ′</td>
</tr>
<tr>
<td>crawl _ext neighborhood</td>
<td>Returns Δ(b), the extended neighborhood of b, as botcargo</td>
</tr>
<tr>
<td>mutual _connect</td>
<td>Connects b to every profile p_i 2 Δ(b) \ B.</td>
</tr>
<tr>
<td>harvest_data</td>
<td>Reads all accessible information of every profile p_i 2 Γ(b), and returns it as botcargo</td>
</tr>
</tbody>
</table>
Economic Analysis
Research Question

• Is it economically feasible for a botherder to operate an SbN?
  – What is the cost structure?
  – How many users to infiltrate? (*scale*)
  – How many bots to use? (*size*)
  – How to maximize the profit? (*strategy*)