The Role of the Underground Market in Twitter Spam & Abuse

Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, Vern Paxson

UCB, GMU, ICSI, Twitter
Overview

- Google, Facebook, Twitter dominate Internet usage
  - Increasingly attractive targets for abuse
  - Closed-garden services require credentials

- Proliferation of fraudulent, spam accounts
  - 3% of Twitter accounts fake [Thomas et al. 2011]
  - 1.5% of Facebook accounts fake [Facebook SEC 2012]

- Emergence of underground services selling accounts
  - Abstract away complexities of circumventing automation barriers
Services for Sale

Facebook Accounts
Yahoo! Accounts
Twitter Accounts
Hotmail Accounts

YouTube Accounts
Gmail.com
Tumblr Accounts
Linked In

Pinterest Accounts
Craigslist Accounts
Tagged Accounts
Mail.com
Our Work

1. Organization of underground account market
2. Merchant techniques for circumventing registration defenses
3. Impact of marketplace on Twitter spam
4. Our efforts to disrupt the account market
Advertisements for Accounts

Kamal Kishore
Data Entry, Web Scraping, SEO, Web Development
Username: Kamalkishore
Location: Muzaffarabad, India
Member since: Feb 2008
We have 4 year working experiences of special areas such as Data Entry, Market Research, Internet Marketing, Social Media Marketing, and Search Engine Optimization (SEO), Web Design. We have been able to grow and expand my knowledge and skills. We provide high quality results for my client 100% Satisfaction.

Reputation:
4.8
(285 reviews)
6.9
[see more]

My activity:
My skills:
Completion Rate 68%
Data Entry 28.6%

buy twitter accounts

About 178,000,000 results (0.24 seconds)

Buy Twitter Accounts | Twitter Accounts in Bulk
buytwitteraccounts.org/Share
We are selling bulk of twitter accounts for your business purpose. Hurry Up!!

Buy Twitter Accounts
buytwitteraccounts.info/
When you Buy Twitter Accounts, you are guaranteeing that you get HUGE ...

Buy Verified Twitter Accounts With Paypaul or Liberty Reserve at ...
We're the only bulk account provider, who sell 7 kinds of Twitter.
Infiltrating the Marketplace

- Track 27 merchants selling Twitter accounts
- Purchase 120K accounts, ~$5,000
  - Bi-weekly purchases from June, 2012 – April, 2013

PayPal | WebMoney | MasterCard | VISA
Market Stats

Price: $0.04  Median account price

Delivery: 1\text{ day}  Median time before accounts arrive

Fraud: 13\%  Accounts are resold, accessed after sale
## Price Comparison

- Prices from buyacccs.com

<table>
<thead>
<tr>
<th>Web Service</th>
<th>Price per Thousand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotmail.com, resale*</td>
<td>$2.00</td>
</tr>
<tr>
<td>Hotmail.com</td>
<td>$4.00</td>
</tr>
<tr>
<td>Yahoo</td>
<td>$6.00</td>
</tr>
<tr>
<td>Twitter</td>
<td>$20.00</td>
</tr>
<tr>
<td>Google (PVA)**</td>
<td>$100.00</td>
</tr>
<tr>
<td>Facebook (PVA)**</td>
<td>$100.00</td>
</tr>
</tbody>
</table>

* Resale indicates account was previously used in another activity
** PVA indicates a phone verified account; challenge response text to cell phone
Abuse Safeguards

- Existing defenses against automation:
  - IP blacklisting, throttling
  - Email challenge-response
  - CAPTCHAs

- Merchants readily circumvent these protections
Evading Blacklisting

- Purchased accounts with unique registration IP: 79%
  - Evenly distributed over /16, /24 subnet
  - Spans 164 countries

<table>
<thead>
<tr>
<th>Registration Origin</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>8.50%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>7.23%</td>
</tr>
<tr>
<td>Turkey</td>
<td>5.93%</td>
</tr>
<tr>
<td>Thailand</td>
<td>5.40%</td>
</tr>
<tr>
<td>Mexico</td>
<td>4.61%</td>
</tr>
<tr>
<td>Other</td>
<td>68.33%</td>
</tr>
</tbody>
</table>

Inexpensive hosts from Pay-Per-Install perspective
Email Confirmation

- Accounts with confirmed email: 77%

<table>
<thead>
<tr>
<th>Email Provider</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotmail.com</td>
<td>60.08%</td>
</tr>
<tr>
<td>Yahoo.com</td>
<td>11.57%</td>
</tr>
<tr>
<td>Mail.ru</td>
<td>11.43%</td>
</tr>
<tr>
<td>Gmail.com</td>
<td>1.89%</td>
</tr>
<tr>
<td>Nokiamail.com</td>
<td>0.93%</td>
</tr>
</tbody>
</table>

Email confirmation increases cost of accounts by 20%
CAPTCHA Solution Rates
CAPTCHA Solution Rates

OCR: 7% accuracy
CAPTCHA Solution Rates

Human Solver: 70-100% accuracy
CAPTCHA Solution Rates

92% of fake registrations fail on CAPTCHA
Detecting Fraudulent Accounts

• Develop a fingerprint of fraudulent behavior
  – Account, user-agent naming conventions
  – Sequence of activities upon registration
  – Timing of registration

• Purely based on registration signals
  – No assumption of tweeting, generating relationships

• Train on 120K purchased accounts
Feature Selection

- Automatically generated naming regex

<table>
<thead>
<tr>
<th>Name</th>
<th>Screenname</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Markita Geske</td>
<td>Markitakjccj</td>
<td>ErnestinaGrogger948 @ hotmail.com</td>
</tr>
<tr>
<td>Philomena Hintze</td>
<td>Philomenadidzz</td>
<td>LauretteBabej239 @ hotmail.com</td>
</tr>
<tr>
<td>Enedina Egert</td>
<td>Enedinaymfee</td>
<td>MikeOrtolani901 @ hotmail.com</td>
</tr>
</tbody>
</table>

- Sequence of registration events

Timing = $\delta_{\text{finish}} - \delta_{\text{start}}$
Classifier Performance

Precision: **99.99%**  
Percentage of identified accounts that are spam

Recall: **95.08%**  
Percentage of all* spam accounts identified
Recall Over Time

- Long-term accuracy requires regular purchasing
How Big a Threat?

- Apply classifier to all Twitter accounts registered from April, 2012 – April, 2013

- Detect *several million* accounts
  - Only a fraction of the accounts previously caught

- Market responsible for 10-20% of all detected spam accounts on Twitter
Market Impact on Twitter Spam

Estimated Revenue: $127K-459K
Disrupting the Marketplace

• With Twitter’s help, suspend all several million accounts we flag as fraudulent

• Iterative process, monitor false postives
  – Precision: 99.9942%

• Monitor market fallout immediately after
Merchant Reactions

“Временно не продаем аккаунты Twitter.com

(Temporarily not selling Twitter accounts)

buyaccs.com
April 6, 2013
All of the stock got suspended ... Not just mine .. It happened with all of the sellers .. Don’t know what twitter has done ...

buyaccountsnow.com
April 10, 2013
Market Fallout, Recovery

- Immediately after intervention:
  - 90% of purchased accounts suspended on arrival
- 2 weeks after intervention:
  - 50% of purchased accounts suspended on arrival
  - Newly minted accounts

- Illustrates need for stronger “at-registration” protections
Conclusion

• Thriving underground market for fraudulent accounts
  – Responsible for 10-20% of fake accounts on Twitter
  – Relies on compromised hosts; CAPTCHA services; ease of acquiring emails

• Generates $127K-459K in revenue from Twitter accounts
  – Only a fraction of overall revenue; multiple services abused
  – Fuels more profitable spam enterprises

• Require stronger “at-registration” defenses
  – Preempts challenge of fake followers, favorite spam, @mention spam, #hashtag spam, RT spam