

# Trafficking Fraudulent Accounts

## 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

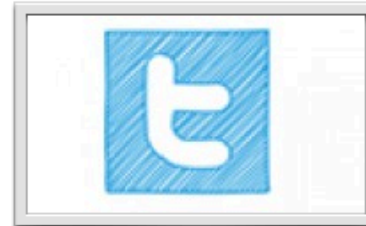
# Services for Sale



Facebook Accounts



Yahoo! Accounts



Twitter Accounts



Hotmail Accounts



YouTube Accounts



Gmail.com



Tumblr Accounts



Linked In



Pinterest Accounts



Craigslist Accounts



Tagged Accounts



Mail.com

# Underground Economy

Products

Phrama/Replica

FakeAV

Click Fraud

Banking Theft

Theft

Dependency

Spamming  
botnets

Banking  
Trojan

PPI services

Exploit kits

Phishing Kits

SEO kits

Packers

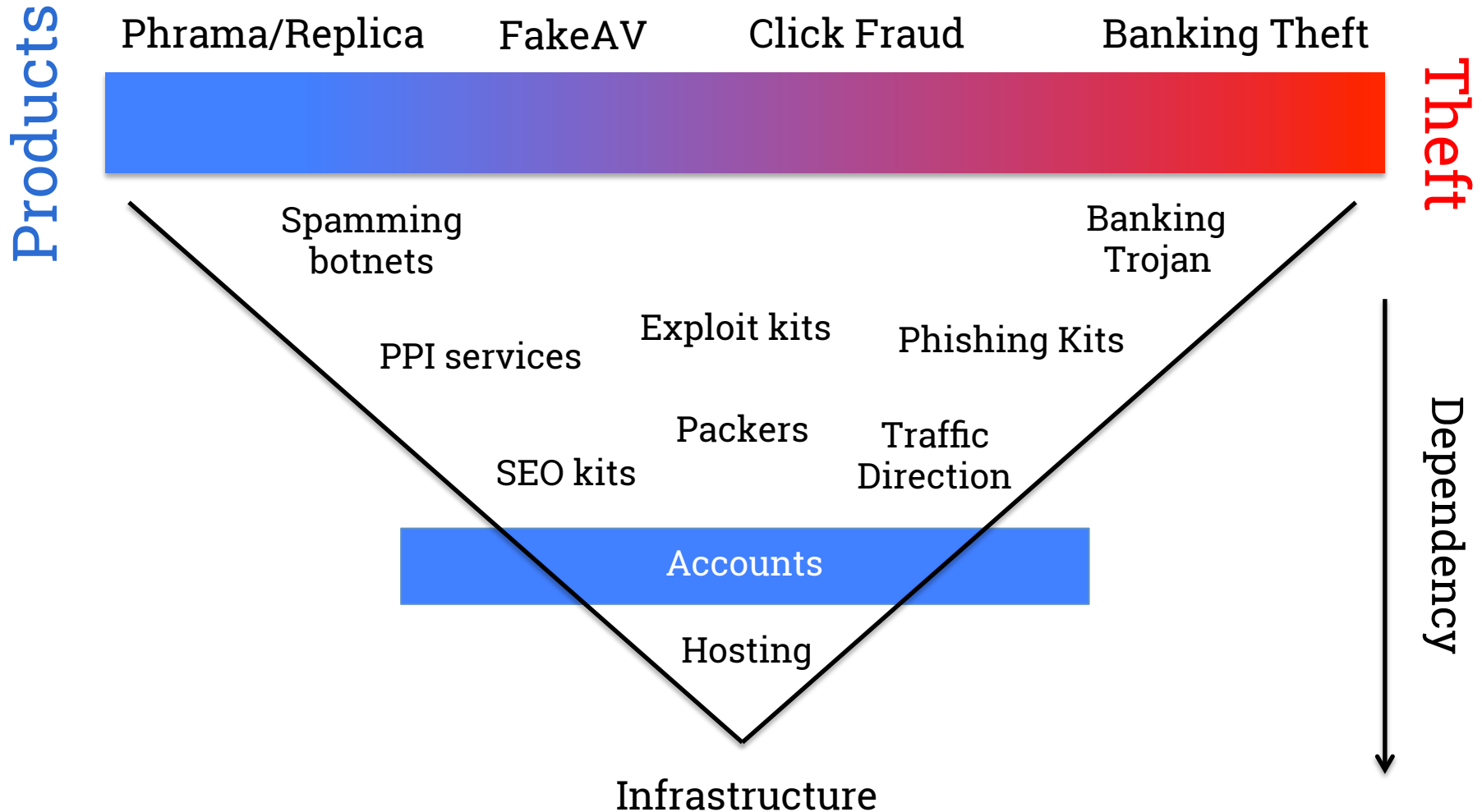
Traffic  
Direction

Hosting

Infrastructure



# Underground Economy



# 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



**Black Hat World**  
BlackHat *Seo Forum*

Forum ▶ The Marketplace ▶ Buy/Sell Services ▶ Best Quality Hotm

Search

Best Quality Hotmail , Yahoo , AOL , Gmx,

09-11-2011, 05:25 PM

Main Menu



buyaccountsnow

Welcome!

We started selling real worldwide Facebook fans and YouTube views! Boost your social presence and increase exposure with our new service.

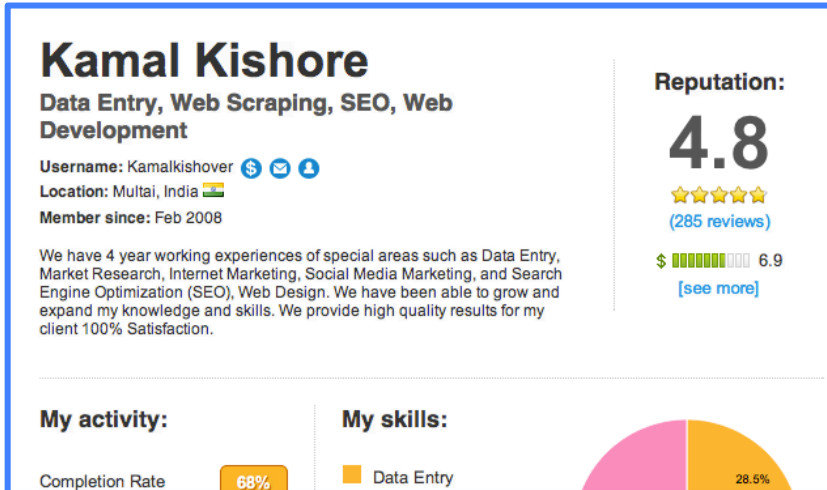
Click HERE for more info!

Facebook Accounts

YouTube Accounts

Buy Accounts

- AOL Accounts
- Craigslist Accounts
- DailyMotion/Tumblr/WordPress Accounts



**Kamal Kishore**  
Data Entry, Web Scraping, SEO, Web Development

Username: Kamalkishover

Location: Multai, India

Member since: Feb 2008

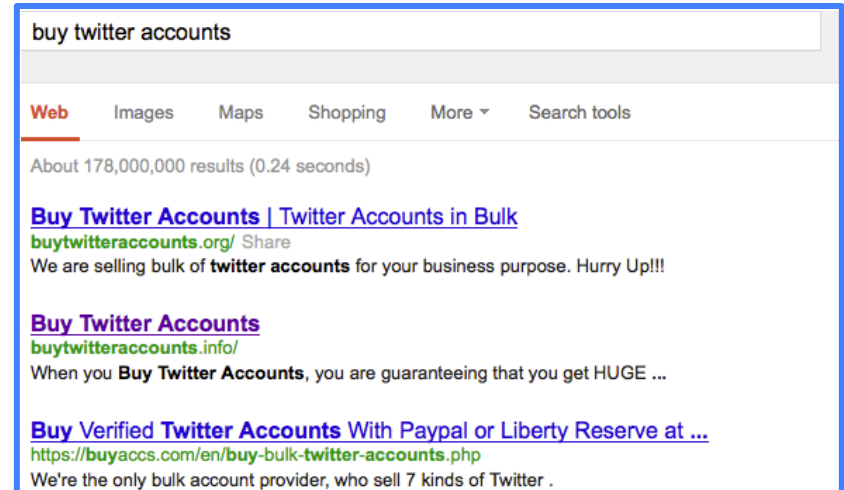
We have 4 year working experiences of special areas such as Data Entry, Market Research, Internet Marketing, Social Media Marketing, and Search Engine Optimization (SEO), Web Design. We have been able to grow and expand my knowledge and skills. We provide high quality results for my client 100% Satisfaction.

Reputation: **4.8**  
(285 reviews)

\$ 6.9 [see more]

My activity: Completion Rate 68%

My skills: Data Entry 28.5%



buy twitter accounts

Web Images Maps Shopping More Search tools

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 Paypal or Liberty Reserve at ...](#)  
<https://buyaccs.com/en/buy-bulk-twitter-accounts.php>  
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**<sup>™</sup>

 **WebMoney**





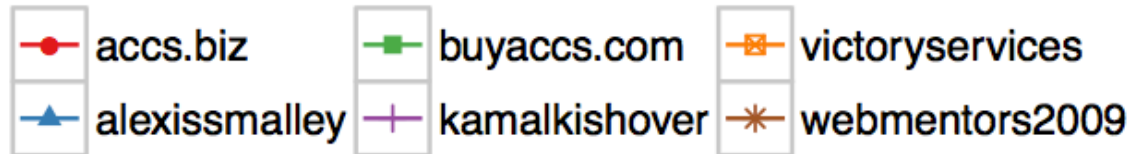
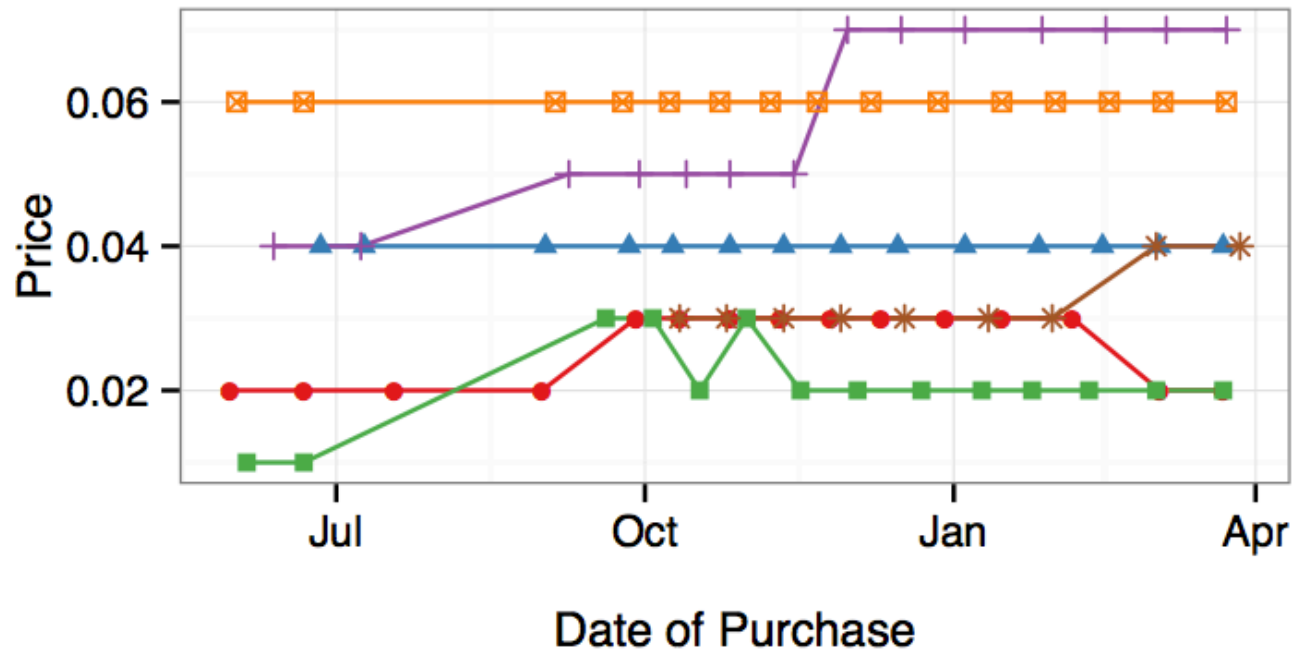
# Market Stats

Price: **\$0.04** Median account price

Delivery: **1day** Median time before accounts arrive

Fraud: **13%** Accounts are resold, accessed after sale

# Prices Over Time



# Price Comparison

- Prices from buyaccs.com

Web Service	Price per Thousand
Hotmail.com, resale*	\$2.00
Hotmail.com	\$4.00
Yahoo	\$6.00
Twitter	\$20.00
Google (PVA)**	\$100.00
Facebook (PVA)**	\$100.00

\* Resale indicates account was previously used in another activity

\*\* PVA indicates a phone verified account; challenge response text to cell phone

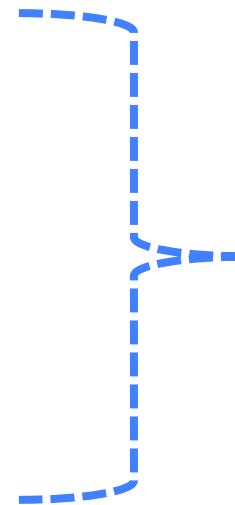
# Abuse Safeguards

- 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

Registration Origin	Popularity
India	8.50%
Ukraine	7.23%
Turkey	5.93%
Thailand	5.40%
Mexico	4.61%
Other	68.33%



Inexpensive  
hosts from  
Pay-Per-Install  
perspective

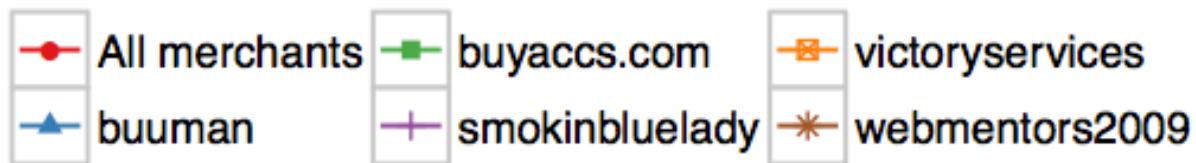
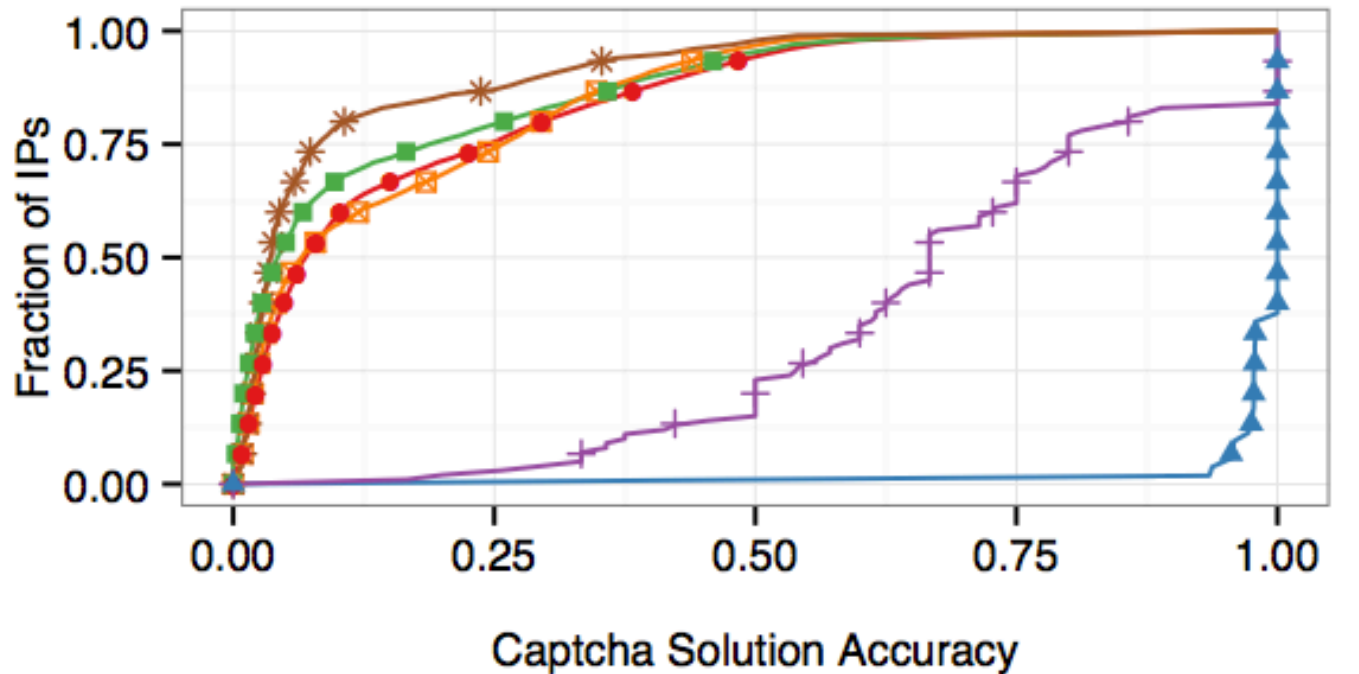
# Email Confirmation

- Accounts with confirmed email: 77%

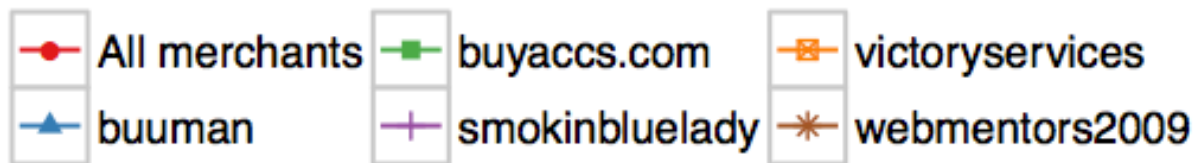
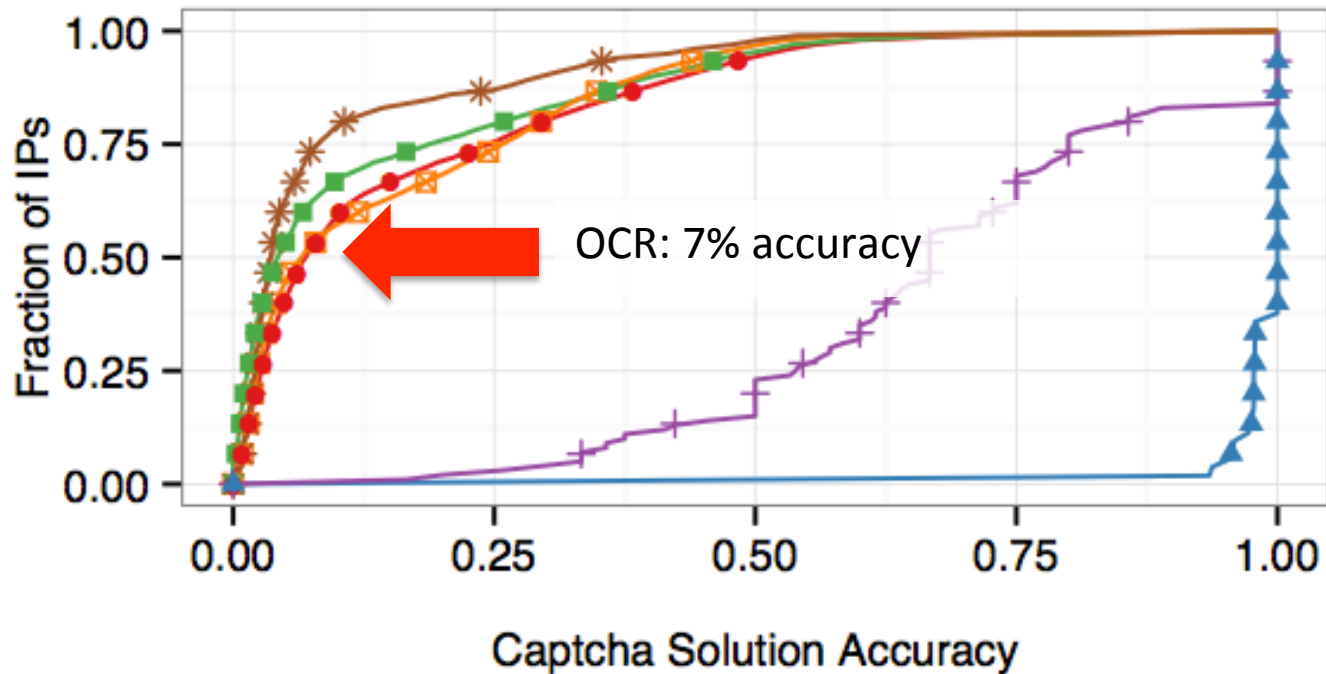
Email Provider	Popularity
Hotmail.com	60.08%
Yahoo.com	11.57%
Mail.ru	11.43%
Gmail.com	1.89%
Nokiamail.com	0.93%

**Email confirmation increases cost of accounts by 20%**

# CAPTCHA Solution Rates

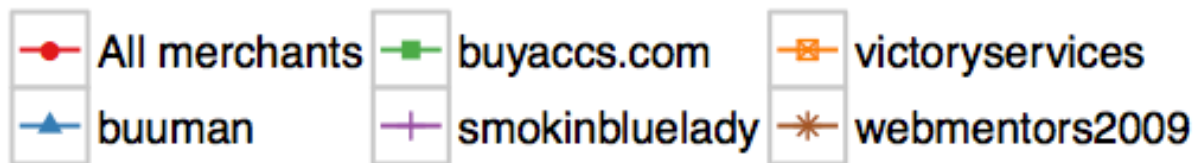
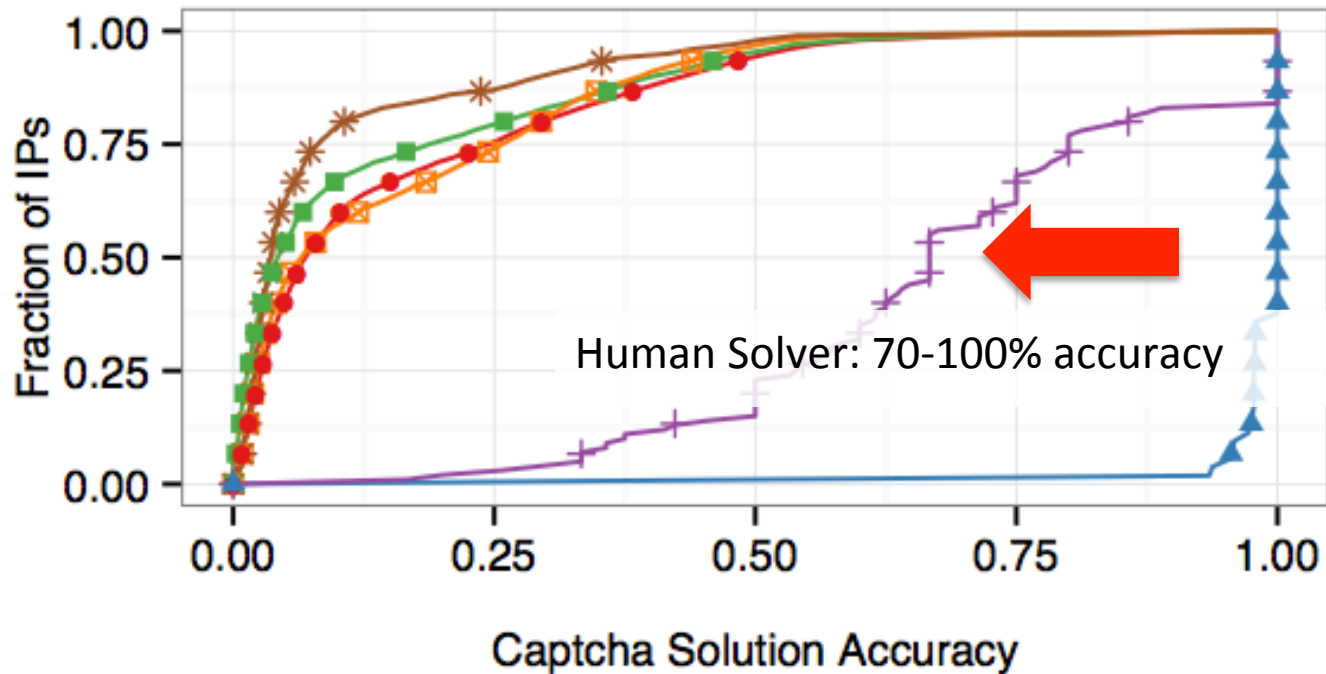


# CAPTCHA Solution Rates

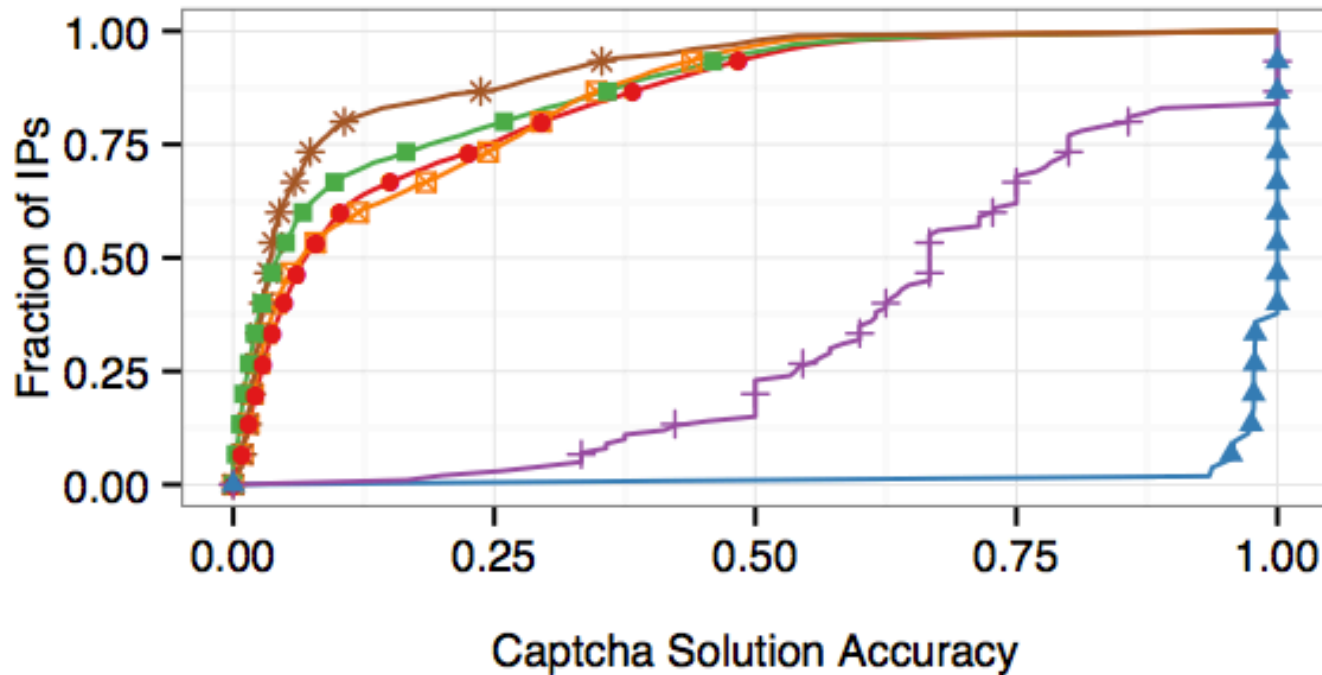




# CAPTCHA Solution Rates



# CAPTCHA Solution Rates



**92% of fake registrations fail on CAPTCHA**

# Detecting Fraudulent Accounts

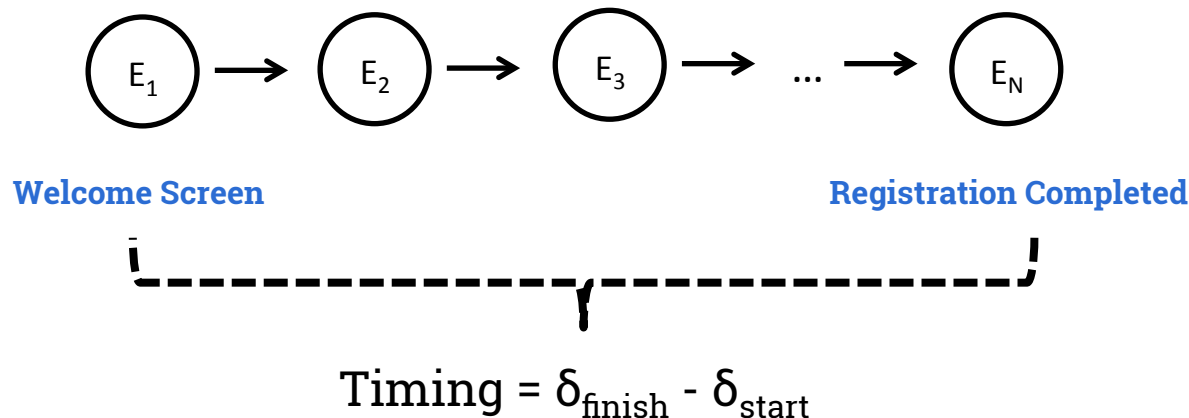
- Develop a fingerprint of fraudulent behavior
  - Account, user-agent naming conventions
  - Sequence of activities upon registration
  - Timing of registration
- Purely based on registration signals
  - No assumption of tweeting, generating relationships
- Train on 120K purchased accounts

# Feature Selection

- Automatically generated naming regex

Name	Screename	Email
<u>Markita</u> Geske	<u>Markitakjccj</u>	ErnestinaGrogger948 @ hotmail.com
<u>Philomena</u> Hintze	<u>Philomenadidzz</u>	LauretteBabej239 @ hotmail.com
<u>Enedina</u> Egert	<u>Enedinaymfee</u>	MikeOrtolani901 @ hotmail.com

- Sequence of registration events



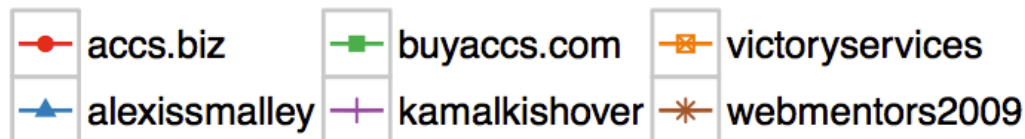
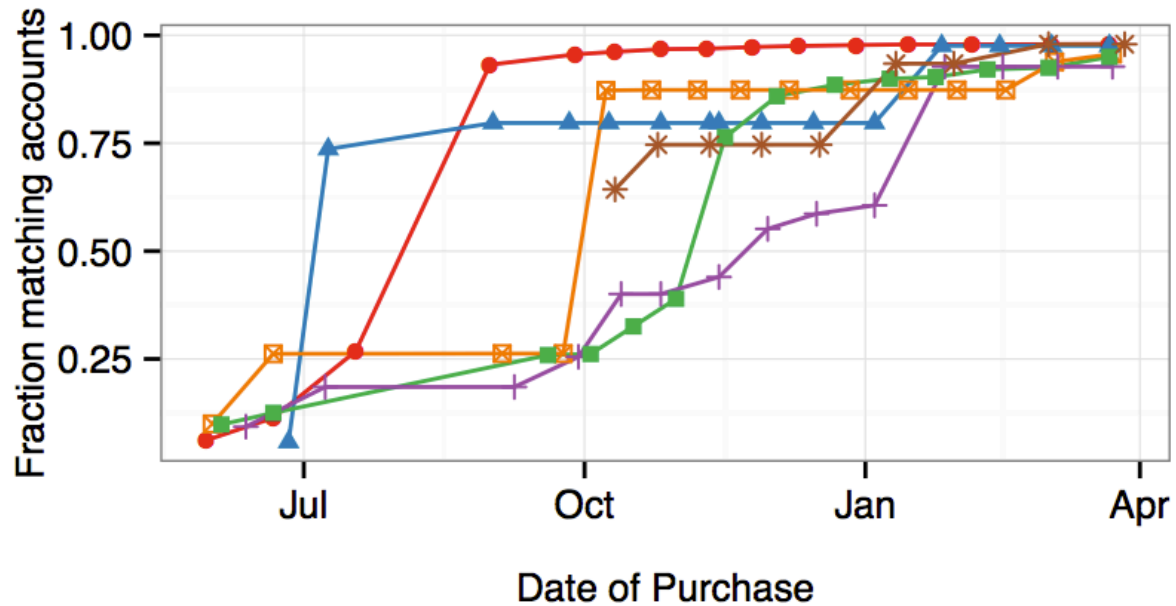
# Classifier Performance

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

**Recall:** 95.08% Percentage of all\* spam accounts identified

# Recall Over Time

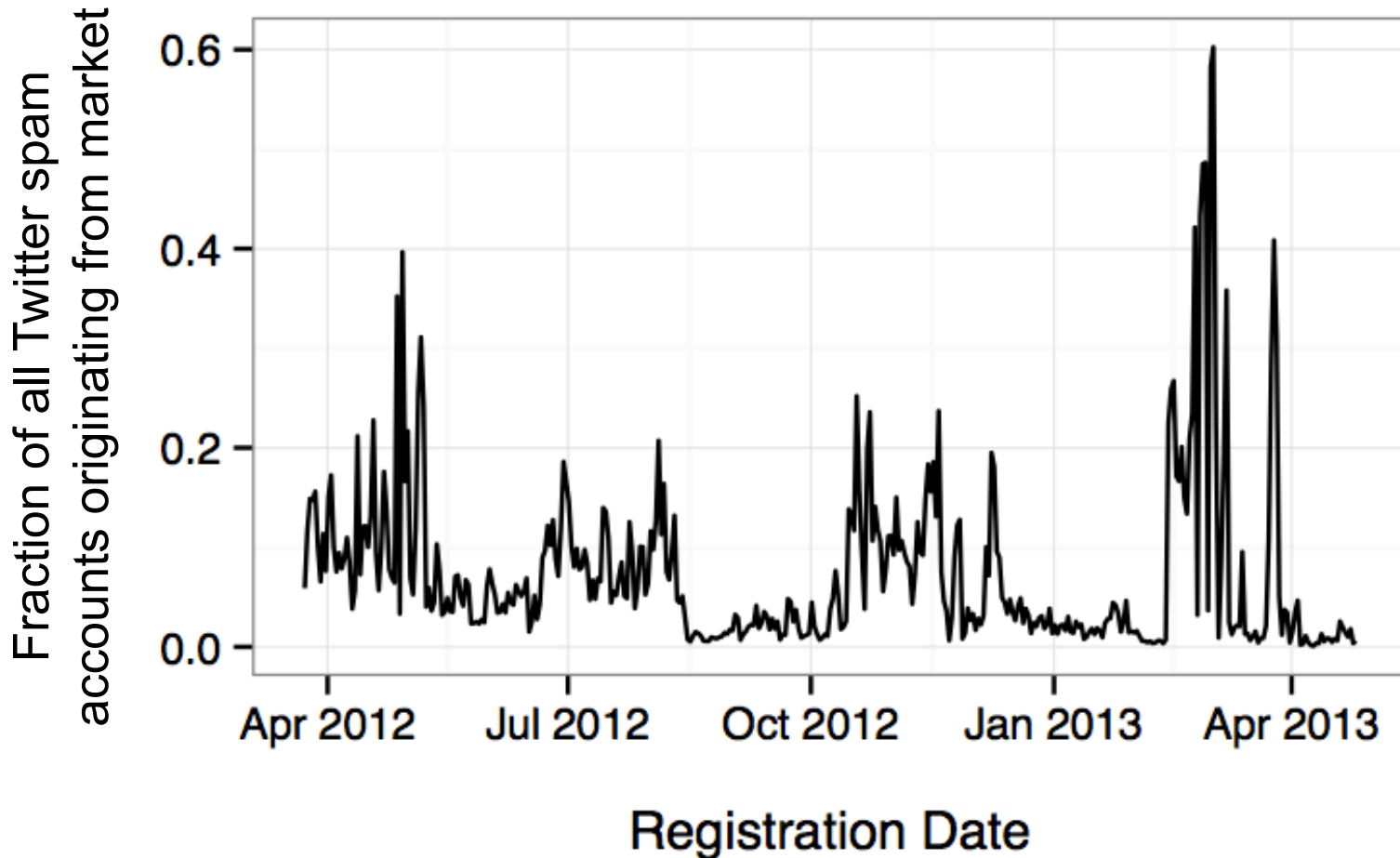
- Long-term accuracy requires regular purchasing



# 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 positives
  - 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

# Merchant Reactions

“

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](http://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