www.BarracudaLabs.com

BARRACUDA LABS

2010 ANNUAL SECURITY REPORT

BARRACUDALABS

FOREWORD

Every year cyber criminals do their part to remind us of the saying that banks are robbed because that is where the money is. As we look back at 2010, we see further evidence of the attackers remaining nimble to focus on the avenues that lead to more money. In this report, we start with the reality that spam volumes dropped in half in the second half of 2010. We then look to other areas where attackers have shifted their attention.

Facebook has become a favorite hunting ground for malicious and spammy activity. Not only has Facebook grown to over 600 million users, but also users spend a tremendous amount of time on the site. This provides a large attentive audience for attackers and they have shown remarkable creativity in pursuing this opportunity. Similarly Twitter continues to be an attractive destination for attackers. While the growth rate of Twitter has slowed, existing users are getting more engaged. As such, attackers have increased their efforts there.

Outside of social networks, we continue to see attackers reach users by search engine malware and by compromising legitimate sites. We look at both sides of the site compromise issue--how do you protect users from visiting infected sites and how do you protect a site from being compromised. We see that while many companies have efforts in place to protect their user base, many companies are not yet actively protecting their Web application infrastructure.

As a community we often point to the need for user education as the missing component; however, the levels of social engineering involved in today's attacks suggest that we must continue to elevate our technological approaches. The social and search vectors along with driveby download capabilities often give the end-user little to no room to affect the outcome. The research community must continue to build innovative defenses and the industry must make efforts to increase the deployment rates of defenses.

Paul Judge, PhD
Chief Research Officer
Barracuda Networks Inc.

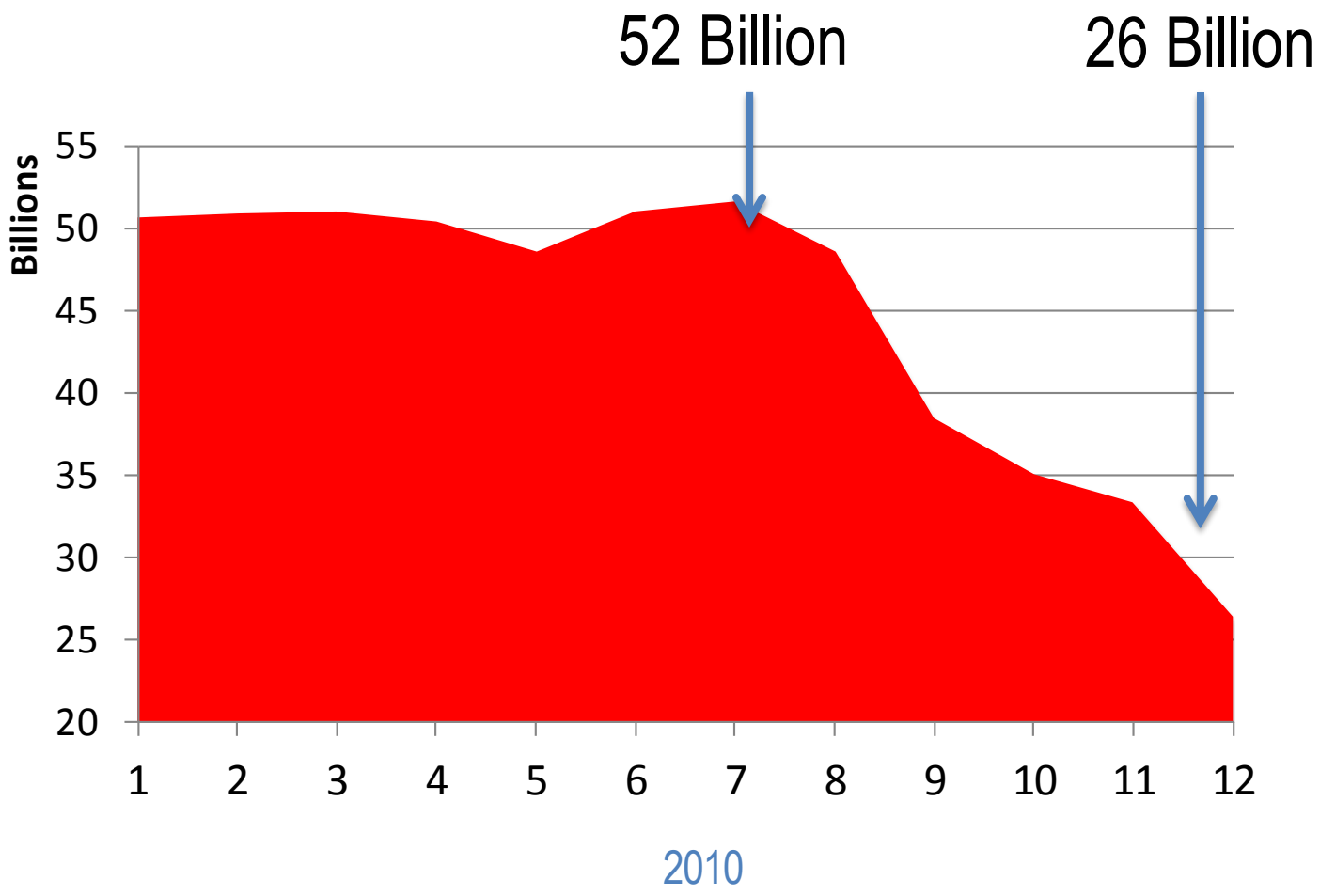
CONTENTS

EMAIL THREATS

WHAT CHANGED IN 2010

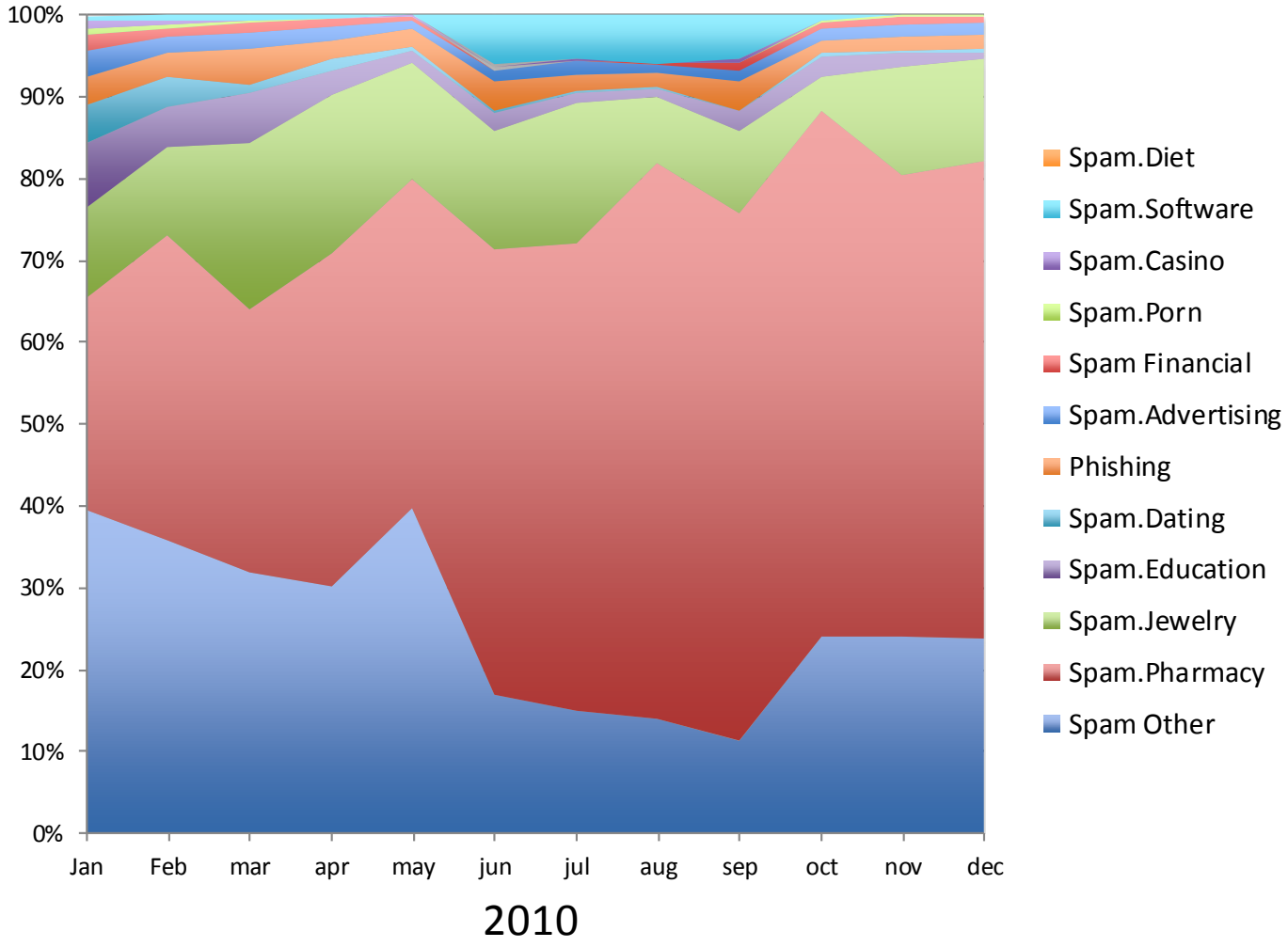
Half of the Spam Disappeared

Attackers more aggressively target the Web



Top Categories of Spam

Pharmaceutical and jewelry lead



SEARCHING FOR MALWARE

A COMPARATIVE STUDY

INTRODUCTION

With search volumes at 88 billion per month on Google sites, 24 billion per month on Twitter, 9 billion per month on Yahoo sites and 4 billion per month on Microsoft sites, search engines are ripe for attackers to leverage for profit.

The goals of this work are to analyze trending topics on search engines, understand the scope of the problem and identify the types of topics used by malware. We first did this measurement in June 2010 and then again in December 2010. The amount of malware found daily increased 55% from 145.7 to 226.3. Malware also was more evenly distributed across the different search engines at the end of the year. In June, Google was crowned "King" of malware, containing 69% of the malware. By December, that number decreased by 45% to Google containing 38% of the overall malware. This shows that attackers have not only increased the amount of overall search engine malware but also have decided that it is worth targeting other search engines besides Google.

Methodology:
We created a system that gets the set of popular search terms hourly and searches for those terms. It then pulls the set of search results and retrieves the web sites of the results. The system then analyzes the sites for malicious code.

The Data Set

A study in search malware

4	Search Engines (Bing, Google, Twitter, Yahoo)
153	Days
157,154	Popular Topics
36,972,206	Search Results

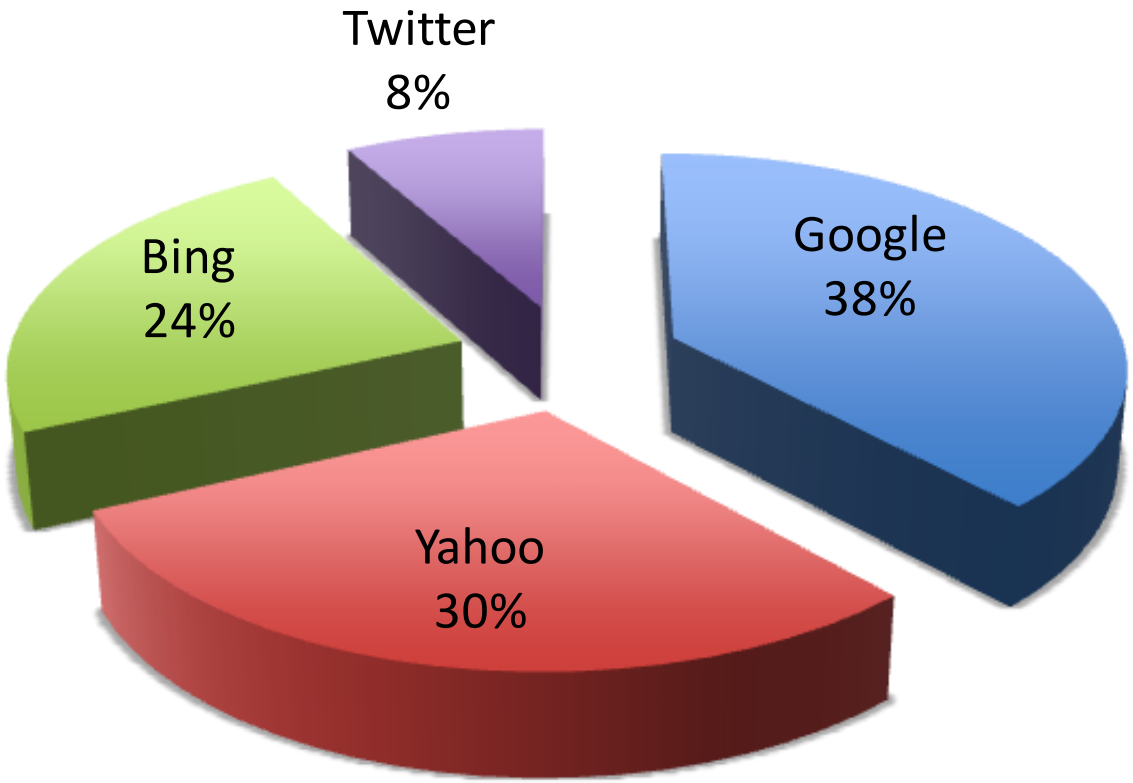
Frequency of Search Engine Malware

Growing problem online

- **34,627** malware samples found
- **1 in 1000** search results lead to malware
- **1 in 5** search topics lead to malware

Total Malware by Search Engine

Google no longer “King”

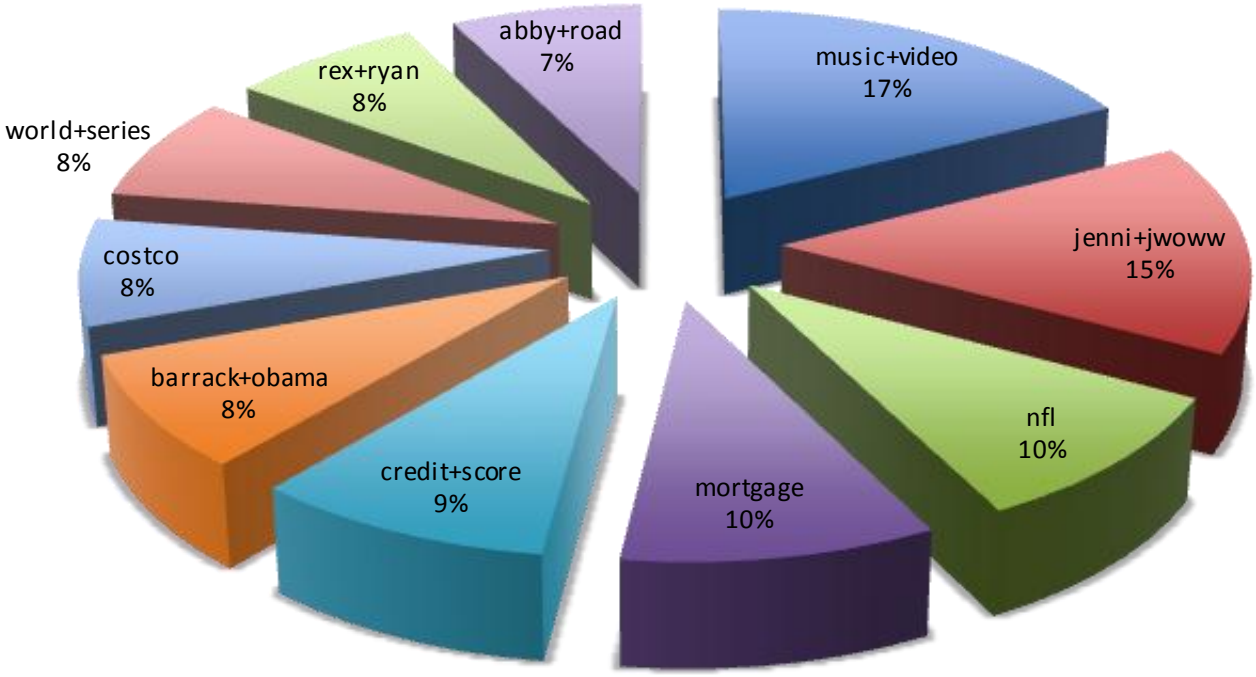


Number 2 Search Term Leading to Malware:

“Jenni J-Woww”

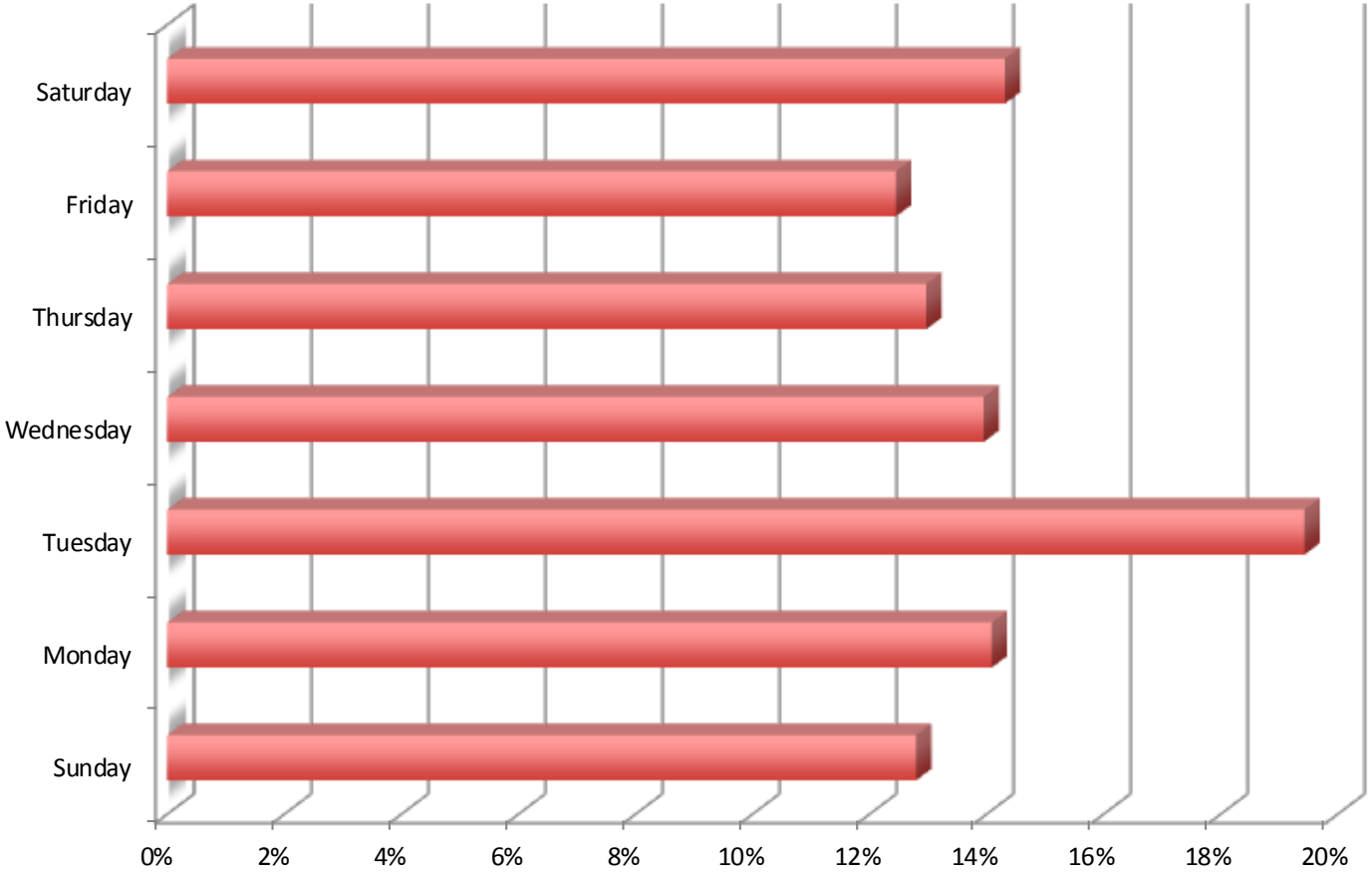
Top Search Terms

That led directly to malware



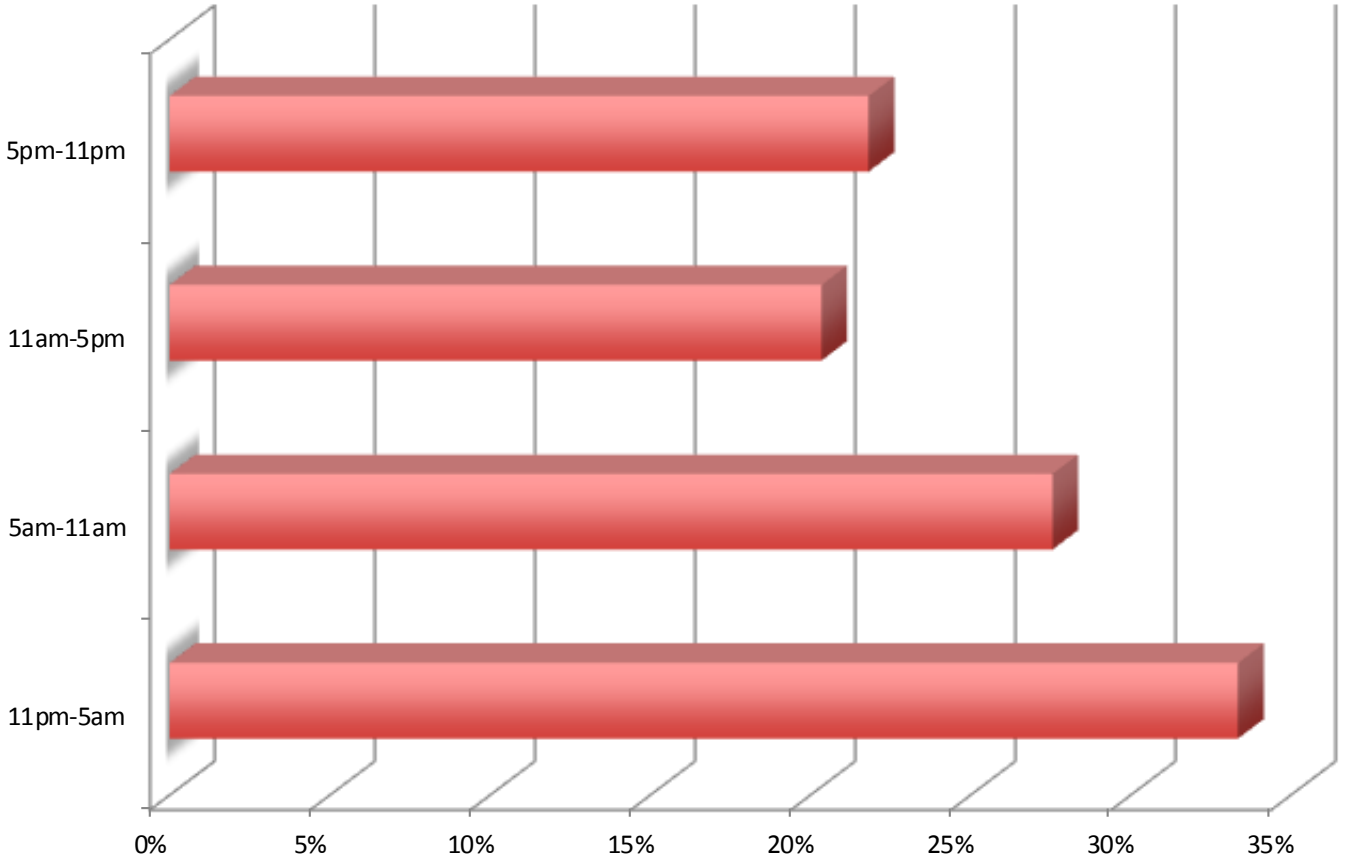
Malware Captured

By day of week

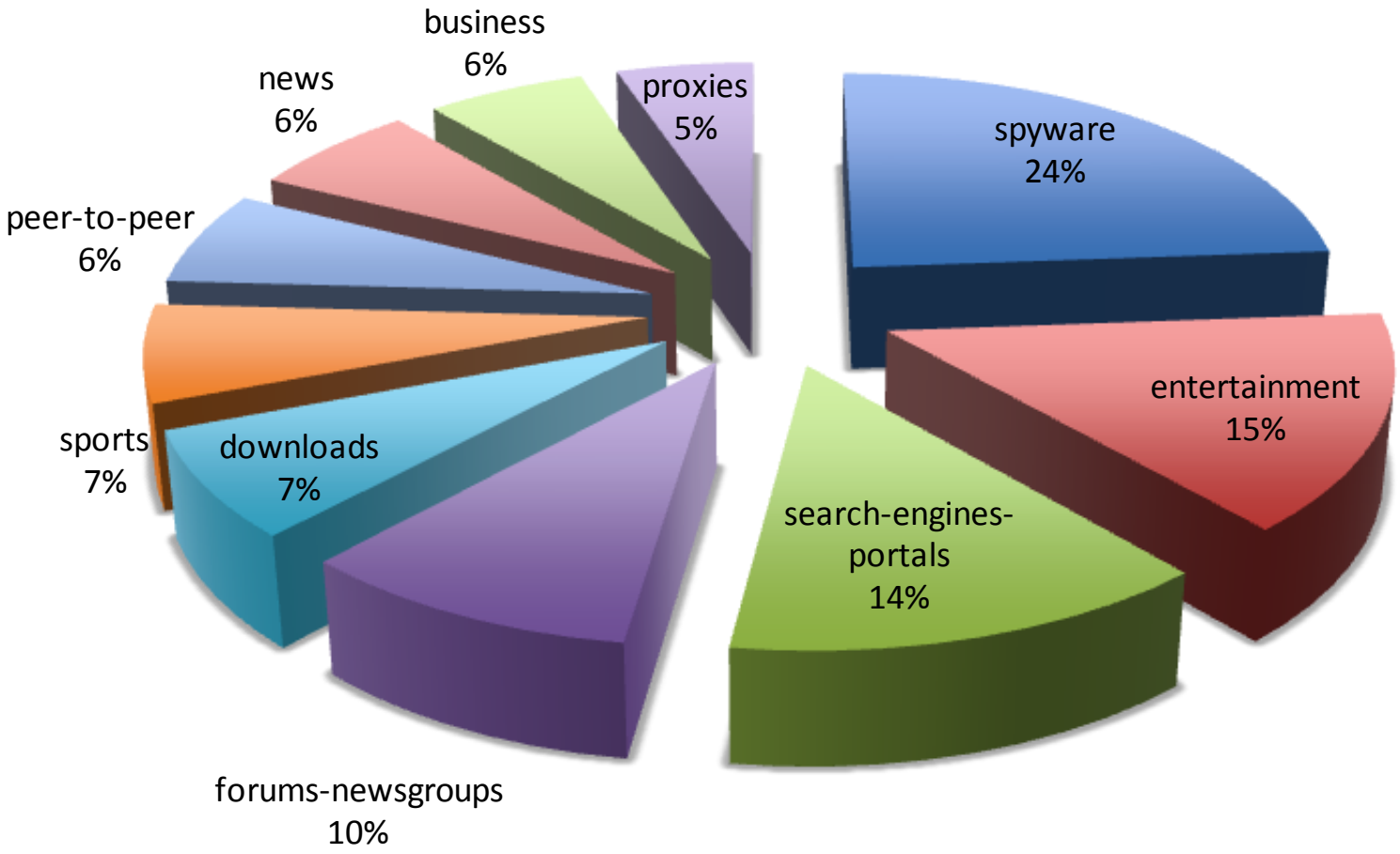


Malware Captured

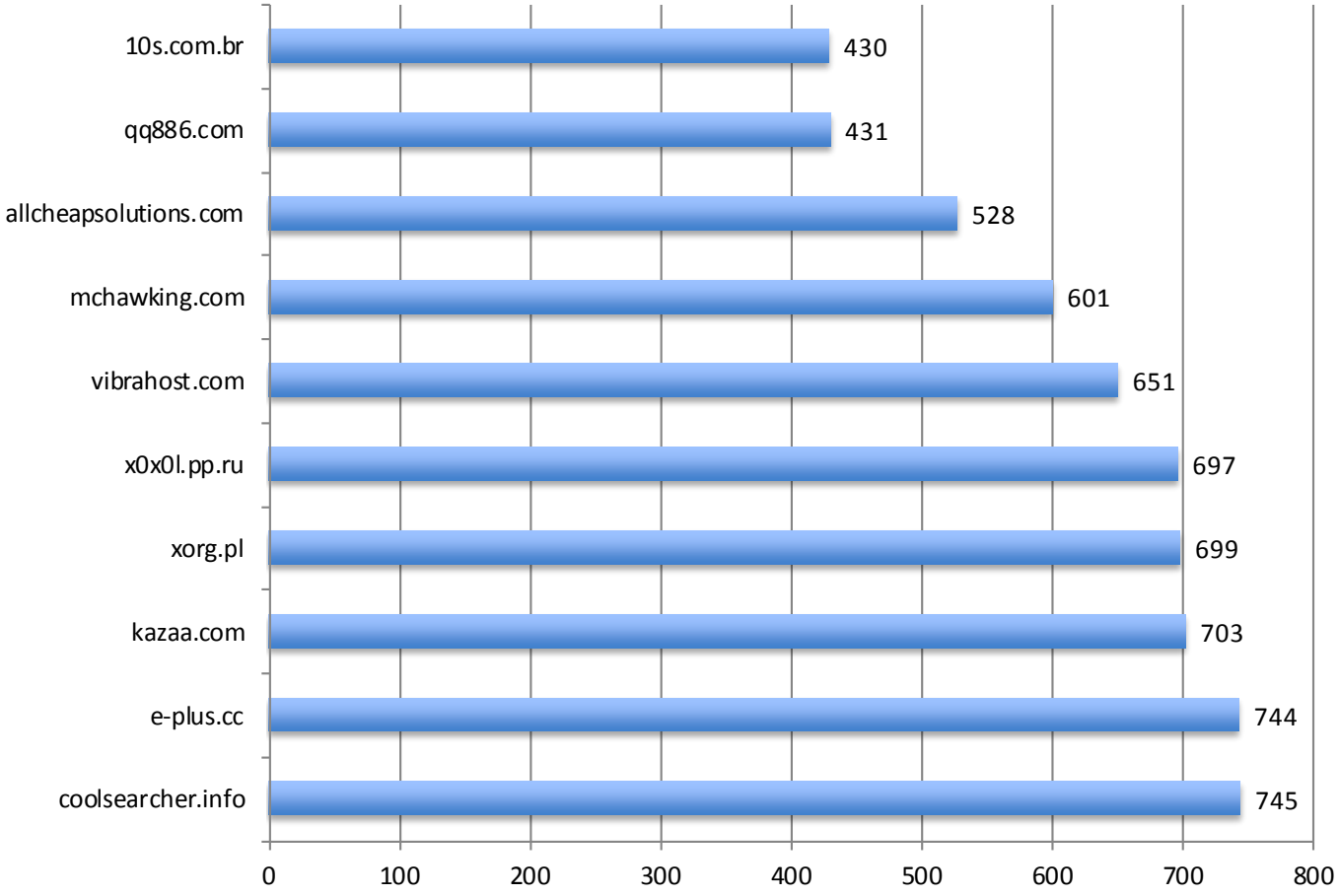
By time of day (EST)



Top 10 Categories
For malware



Top Domains
Hosting malware



So...

what does all of this mean?

Summary
Searching for malware

- Search engine volumes have reached new highs
- Everyday hundreds of pieces of malware are found by simply searching for popular terms
- Search engine ranking and optimization contribute to the effectiveness for attackers

TWITTER

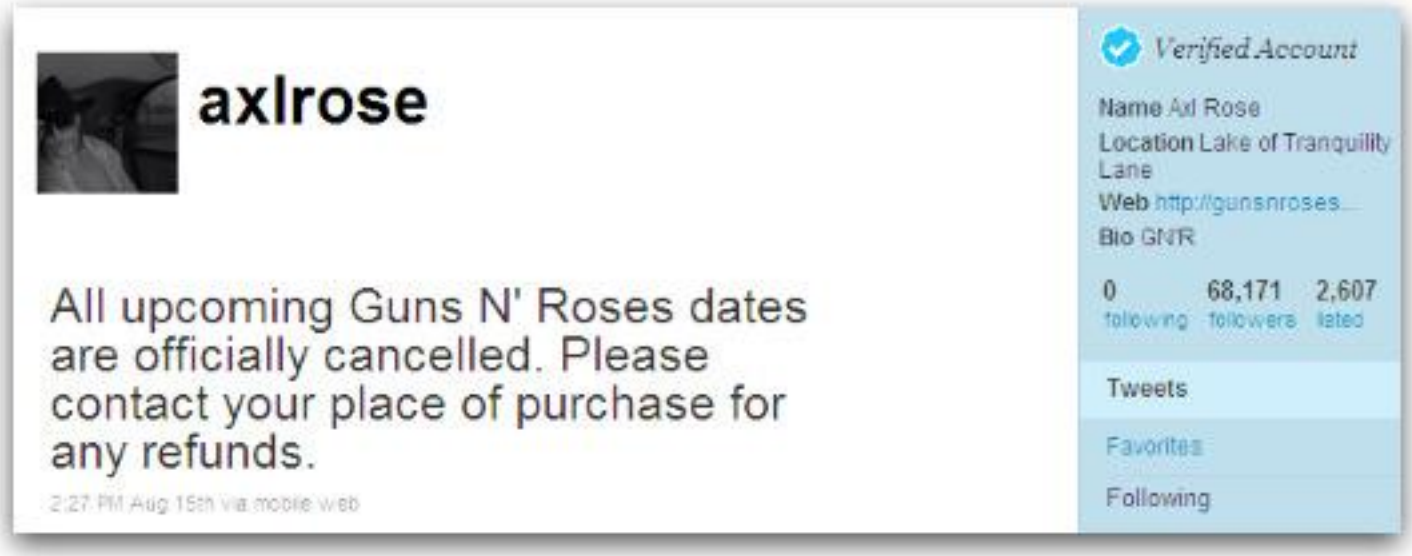
TRENDS & TRACKING

TWITTER

TRENDS & TRACKING

- ACCOUNT HIJACKINGS

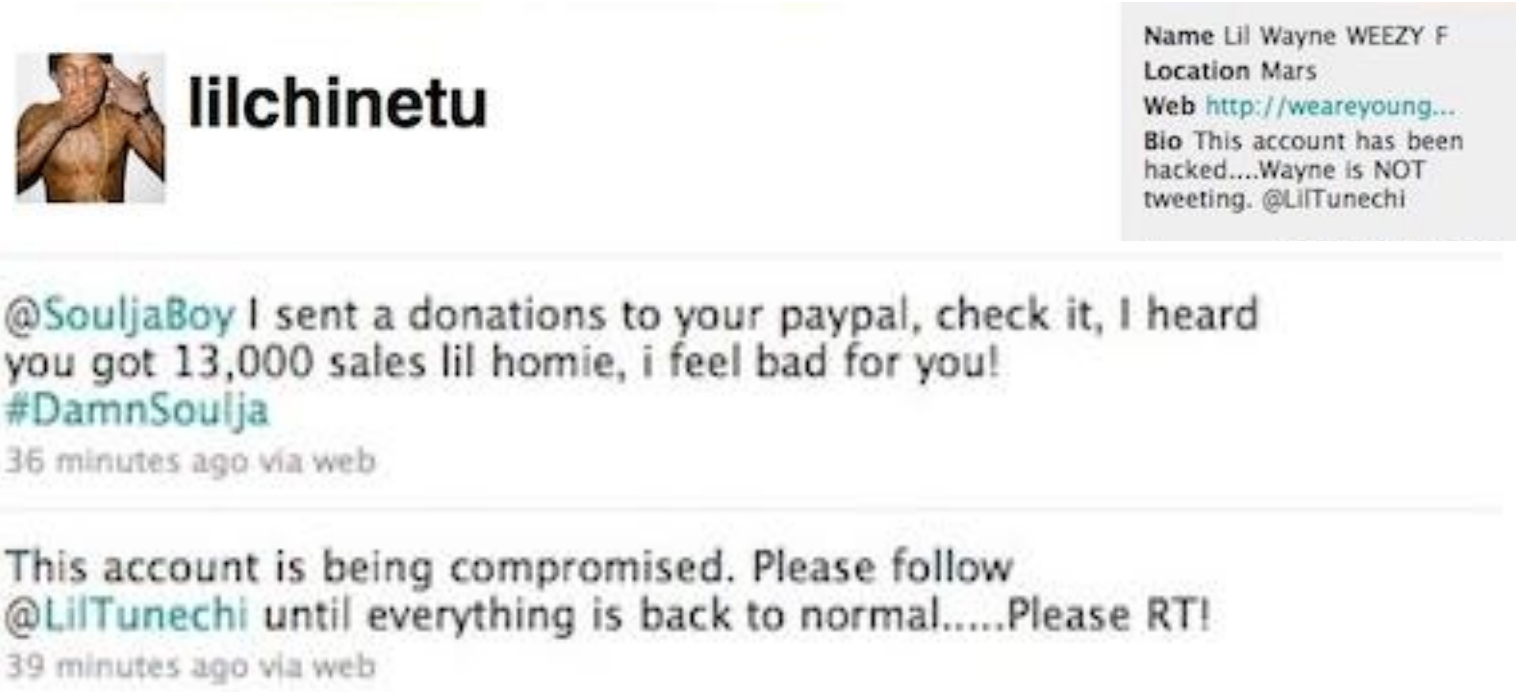
Guns n' Roses Axl Rose



New York Times “The Moment”

- everyone visit http://tinyurl.com/nakedcam for 100% FREE webcam girls/guys doing anything you ask them in the chat, I love it personally.

Lil Wayne


lilchinetu
Name Lil Wayne WEEZY F
Location Mars
Web http://weareyoung...
Bio This account has been hacked....Wayne is NOT tweeting. @LilTunechi
@SouljaBoy I sent a donations to your paypal, check it, I heard you got 13,000 sales lil homie, i feel bad for you! #DamnSoulja
36 minutes ago via web
This account is being compromised. Please follow @LilTunechi until everything is back to normal.....Please RT!
39 minutes ago via web

Corporate America - BP

TWITTER

TRENDS & TRACKING

- SECURITY HOLES

Hacked Servers & Accounts

- Attacker: François Cousteix, 25 yrs old
- April 2009: Broke into internal administration system
- Accessed: Barack Obama, Britney Spears, Ashton Kutcher and others
- March 2010: Sentenced to five months suspended sentence

Force Follow

- May 2010
- ***accept [username]***
- Forces [username] to automatically follow you
- Discovered by 17-year-old Turkish student

onMouseOver – XSS

- September 2010
- Cross-site scripting (XSS)
- Abusers added code that caused people to retweet the original Tweet without their knowledge

CSRF

Malicious Links on Twitter 4 months ago

A malicious link is making the rounds that will post a tweet to your account when clicked on. Twitter has disabled the link, and is currently resolving the issue.

UPDATE Sun Sep 26 18:41:49 UTC 2010: We've fixed the exploit and are in the process of removing the offending Tweets.

Twt.tl – URL shortener

- March 2010
- twt.tl announced
- Link shortening service to help classify malicious URLs

OAuth – Platform Access

- August 2010

- Enables applications to access the Twitter platform on your behalf without ever asking you directly for your password

TWITTER

TRENDS & TRACKING

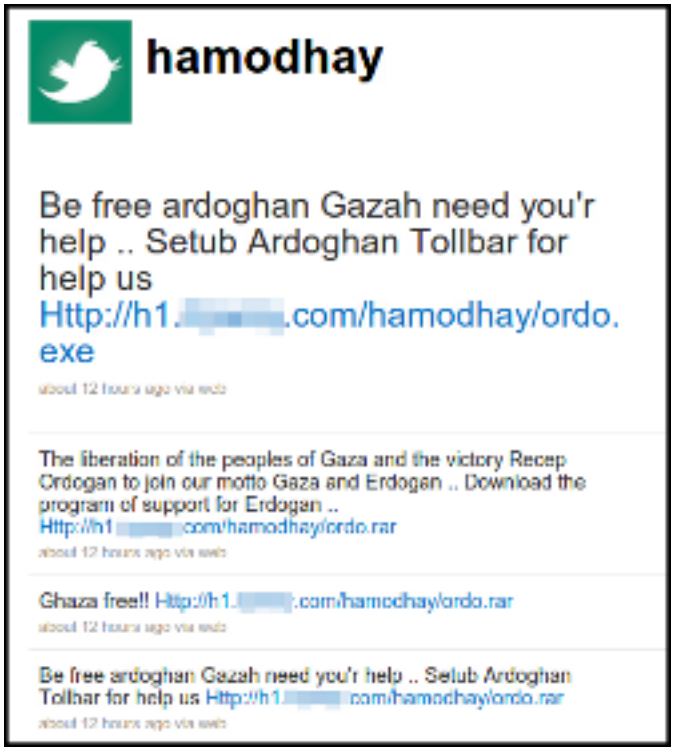
- MALWARE ON TWITTER

“Funniest Video Ever”
Banking Trojan

phylissro	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC Stacey Dash #firstdateturnoffs Projeto Ficha
phylissro	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC Official Twitter App #theuglyfriend Olympic mascots
tristakstp	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC Stacey Dash Bustin Jieber Bustin Jieber
maryroseolaahb	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC #theuglyfriend #theuglyfriend #followerquestion
hyedd	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC Stacey Dash Oil Spill #theuglyfriend
phylissro	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC #firstdateturnoffs Projeto Ficha Stacey Dash
tristakstp	haha this is the funniest video ive EVER SEEN! http://bit.ly/b6Z3BC Stacey Dash Stacey Dash #followerquestion

Source: http://www.f-secure.com

Israeli / Gaza Strip
Bifrost Trojan



- Bifrost Trojan

- Sets up backdoor
- Some install rootkit
- Allows execution of arbitrary code

Source: http://nakedsecurity.sophos.com

Goo.gl Shortener
NeoSploit exploit kit

- December 2010

- Goo.gl shortened links are sent
- Links point to a French Furniture manufacturer
- Several redirects lead to site infected with NeoSploit exploit kit

Goo.gl Shortener
To RogueAV

Source: http://www.securitynewsdaily.com

TWITTER

TRENDS & TRACKING

- REPUTATION SYSTEM

INTRODUCTION

Several years ago, all content on a Web site was produced by the site owner, and users could simply check for that familiar lock at the bottom of the browser in order to feel safe online. However, that has changed dramatically in recent years as user-generated content became mainstream. With hundreds of millions of users behind a single domain, there is a need for online reputation checks to increase overall trust. In reference to Twitter, this user level reputation is needed to understand if an account is good or bad, or if the profile is even real.

RELATED WORK

Social Reputation

The Eigentrust algorithm for reputation management in P2P networks. international conference on World Wide Web 2003.

IP Reputation for Email

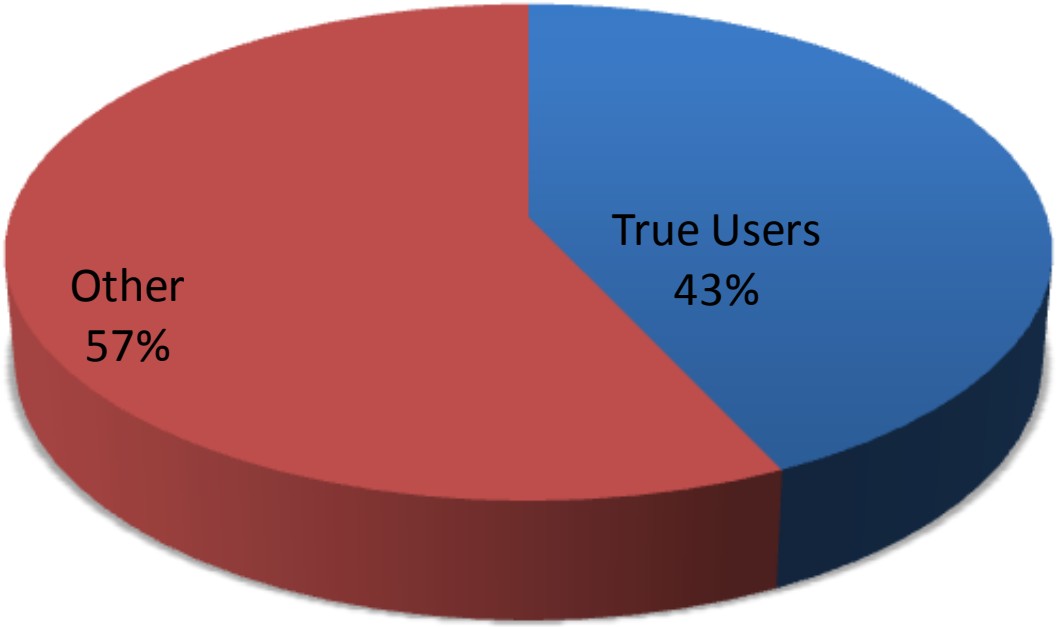
Spam Sender Detection with Classification Modeling on Highly Imbalanced Mail Server Behavior Data. 2008 International Conference on Artificial Intelligence and Pattern Recognition.

URL Reputation

Identifying Suspicious URLs: An Application of Large-Scale Online Learning. Ma et al. International Conference on Machine Learning 2009

TRUE TWITTER USERS

≥10 Followers, Friends, & Tweets



43% of users are True Twitter Users -- compared to 21% in Jan 2010 and 29% in July 2010, showing a much more active user base.

Followers: For every 100 Twitter users…

11 have
0
followers

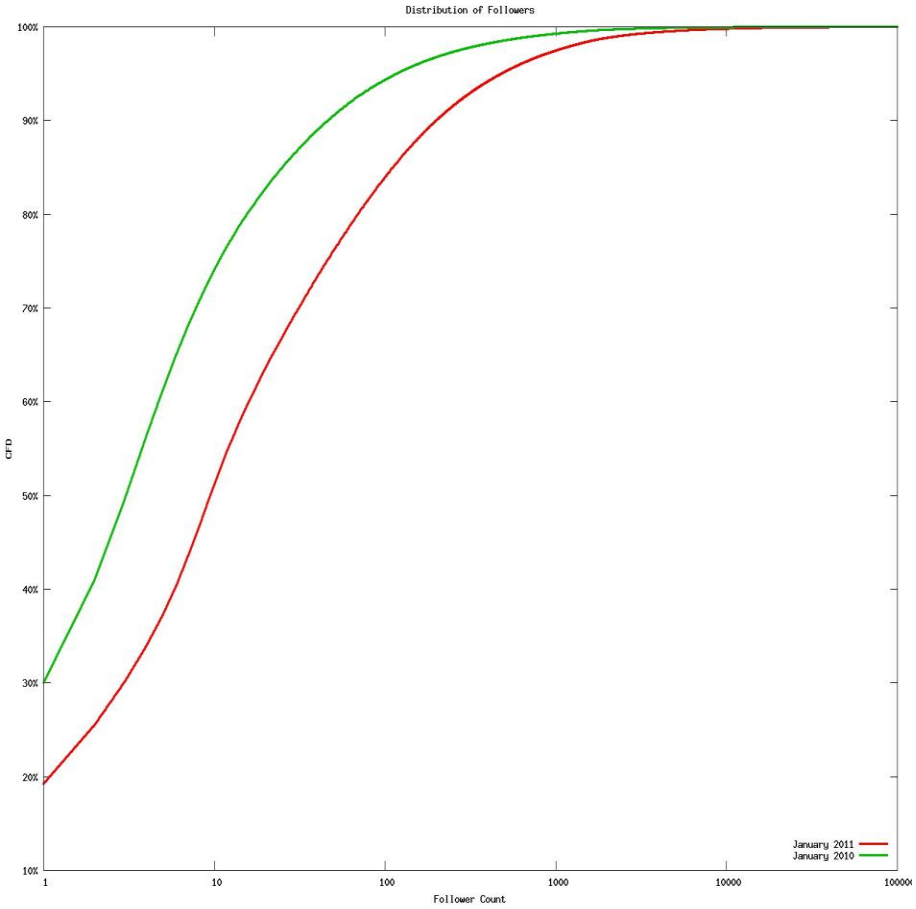
39 have
1-9
followers

33 have
10-99
followers

17 have
100+
followers

Follower Count

- 11% have no followers
  - 30% decrease from July 2010 when it was 15%
- 50% have 10+ followers
  - 51% increase from July 2010 when it was 33%



Friends/Following: For every 100 Twitter users…

16 have
0
friends

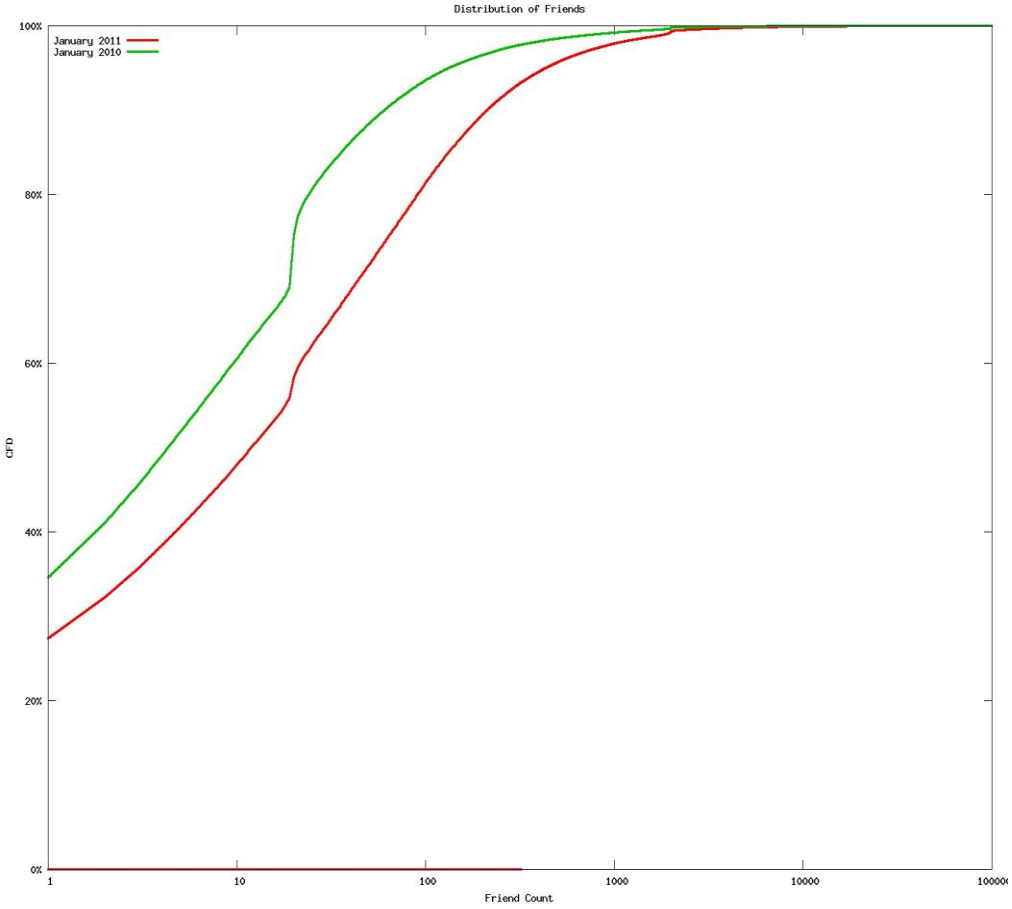
27 have
1-9
friends

40 have
10-99
friends

17 have
100+
friends

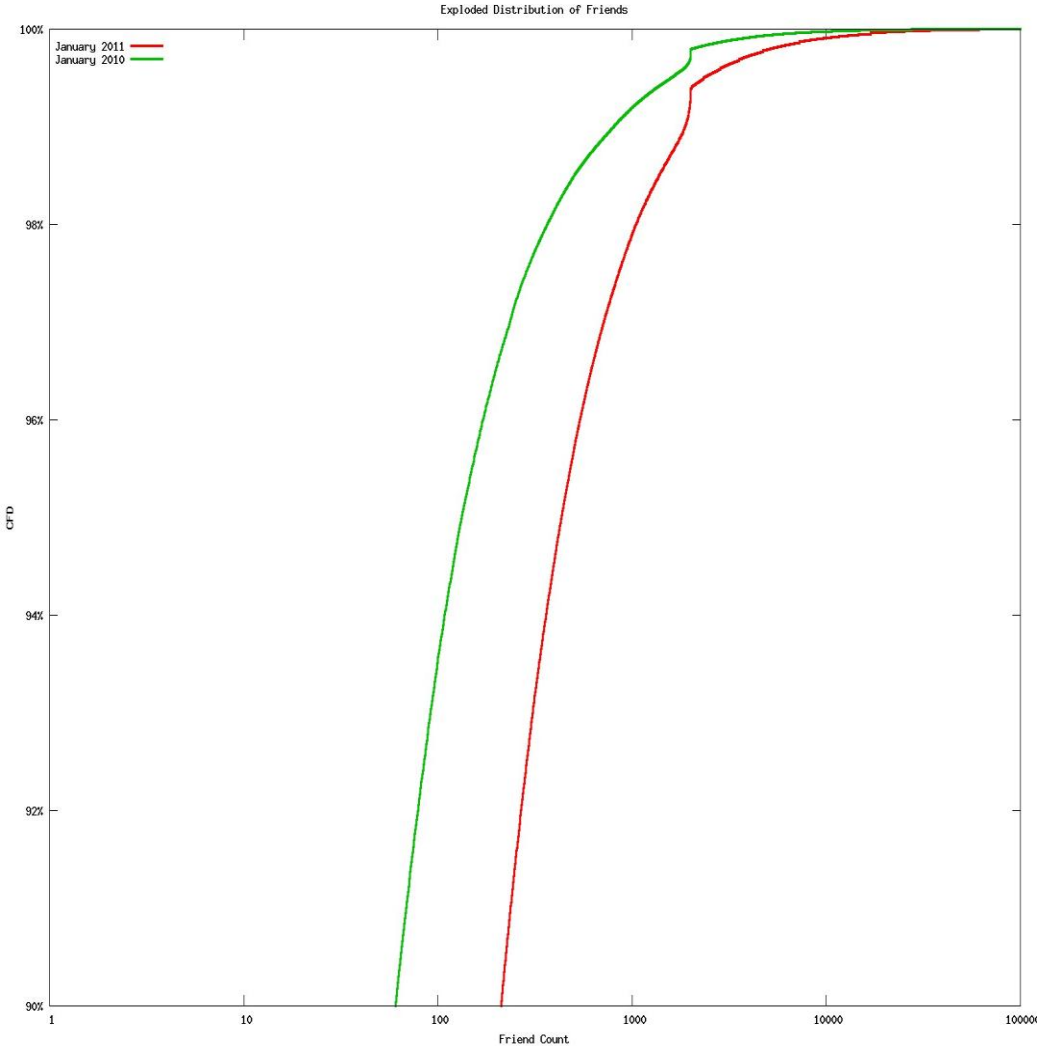
Friend (Following) Count

- 16% following no one
  - 15% decrease from 18.9% in July 2010
- 57% are following 10+
  - 26% increase from 45% in July 2010



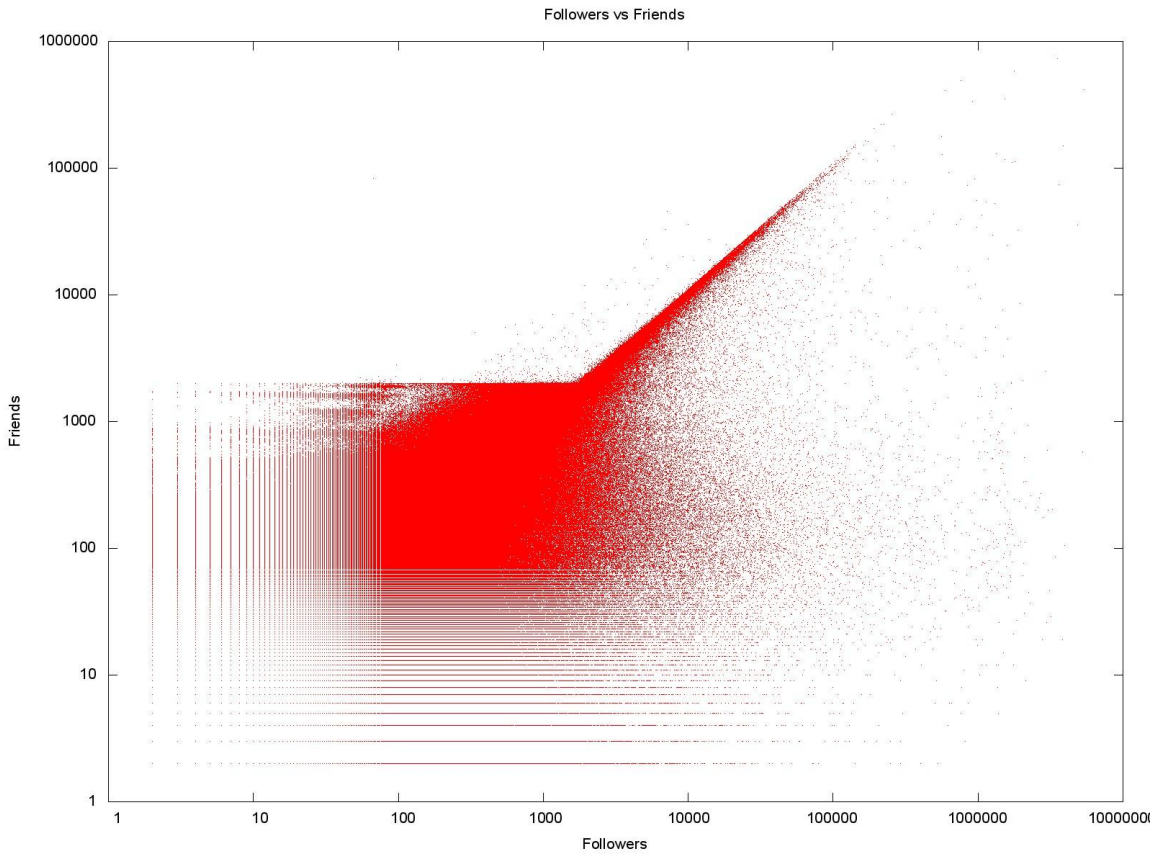
Following Count (>90%)

- >100 17%
- >1000 1%
- > 10000 0.01%



Followers vs. Friends

Comparison or relationship direction



The limitation of following 2,000 people is seen.

Also beyond that there is a strong correlation of accounts that follow their followers.

Friend: Follower Delta

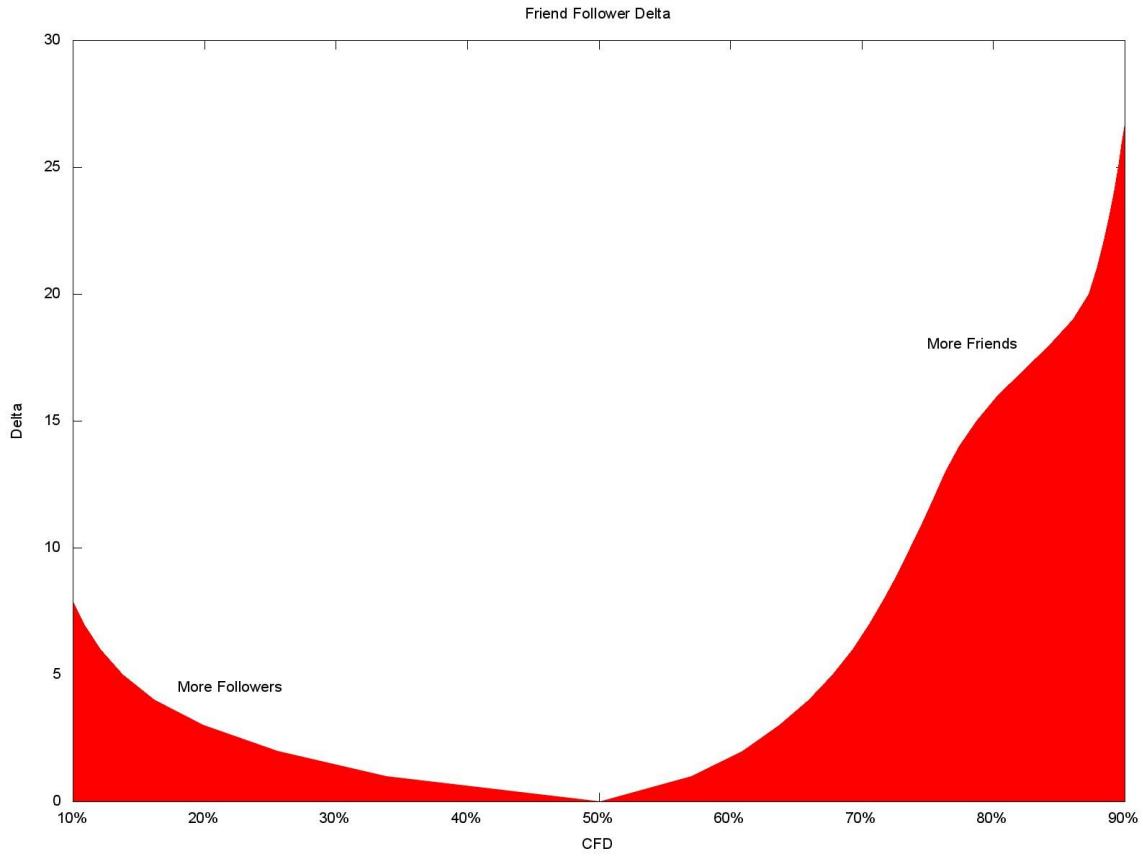
For every 100 Twitter users…

34
have
more
followers

43
have
same
(+/- 5) amount

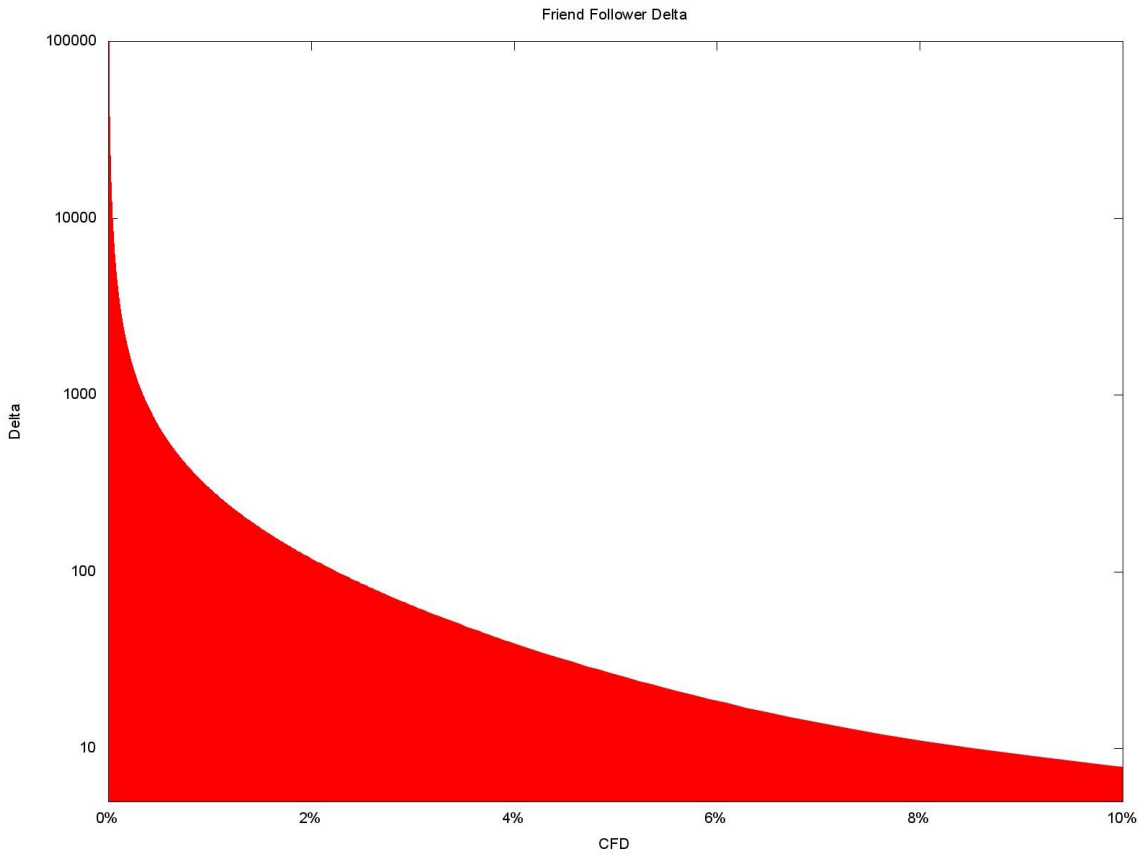
23
have
more
friends

Friend Follower Delta
(10-90%)



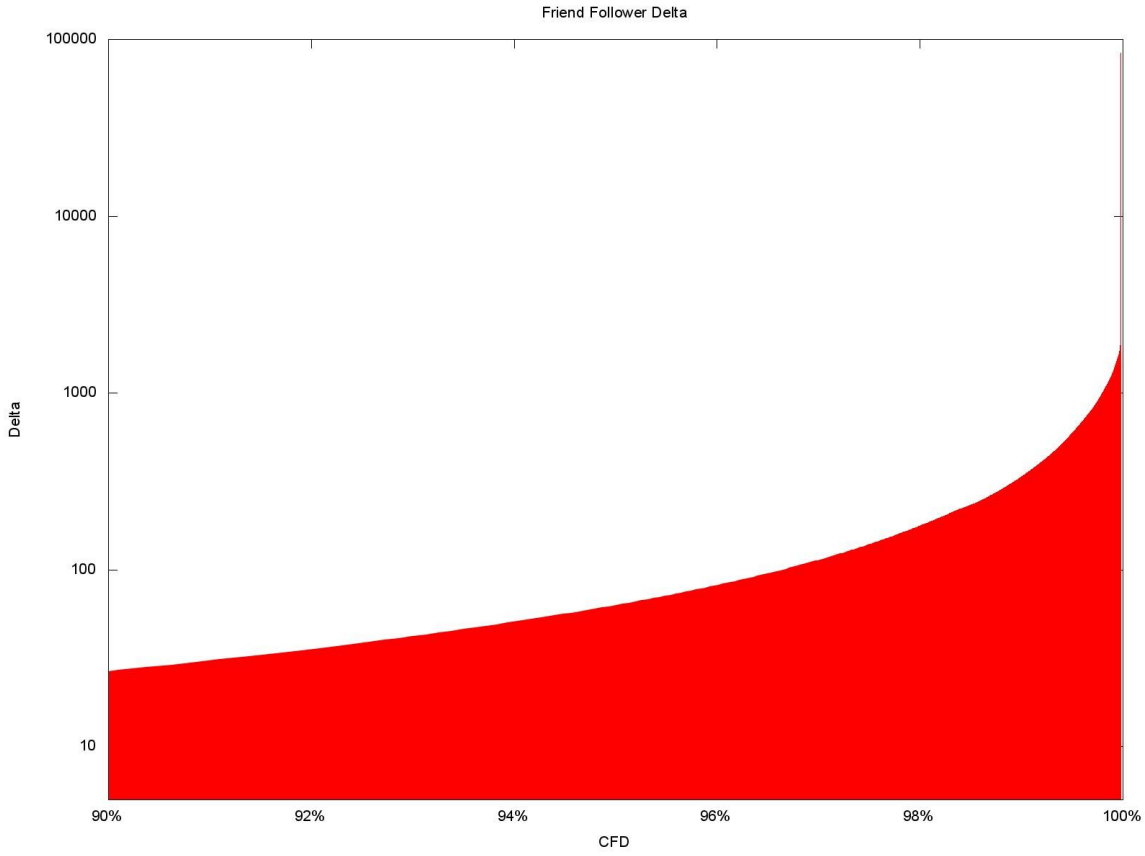
Friend Follower Delta (0-10%)

Bottom 10% have way more followers than they are following ---- Celebrities

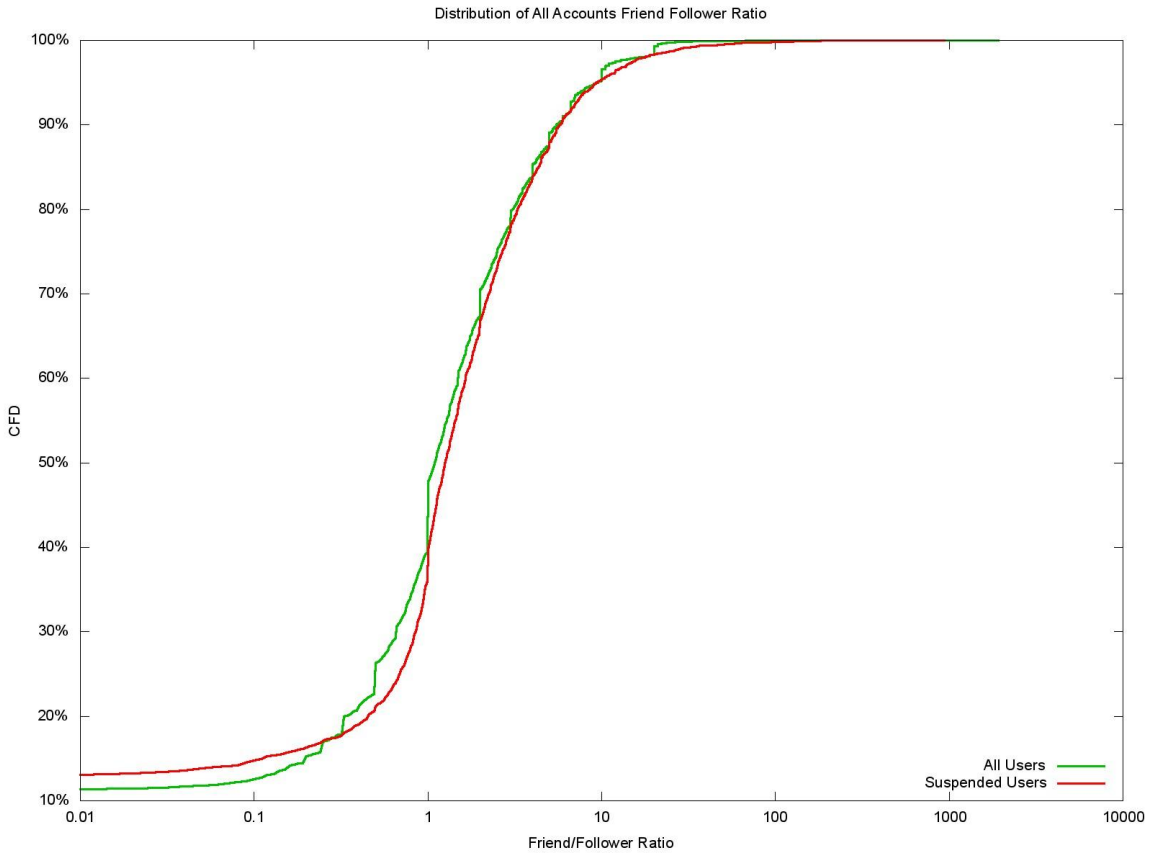


Friend Follower Delta (90-100%)

There's more consumers than producers…
Lot more people who think they know what they are talking about….and these are the ones who don't…

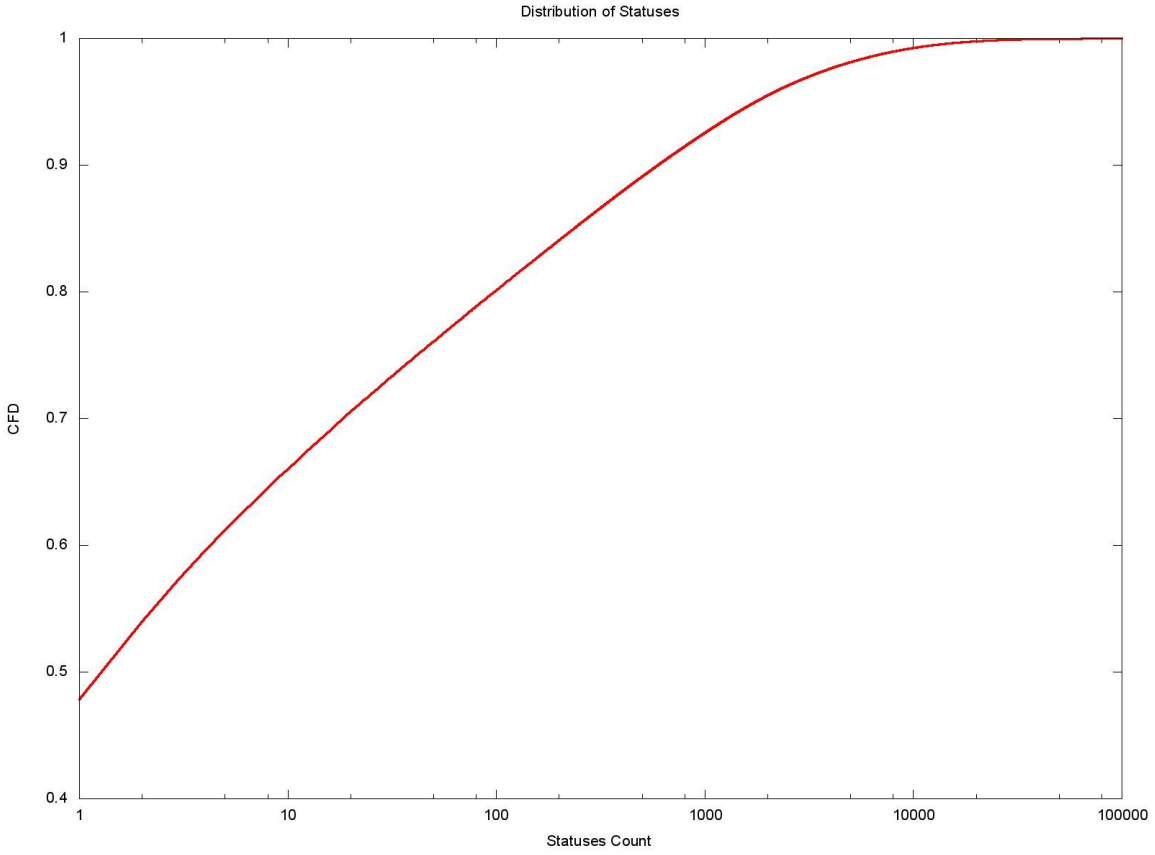


Friend Follower Ratio



Number of Tweets

A view of total tweet volume



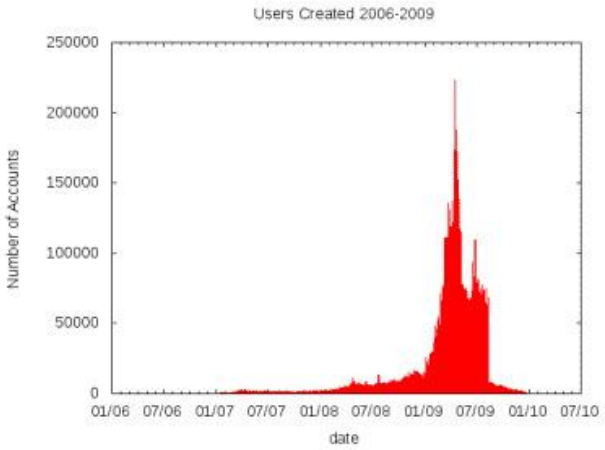
The Dark Side of Twitter

Twitter Crime Rate

Twitter crime rate is the percentage of accounts created per month that are eventually suspended by Twitter.

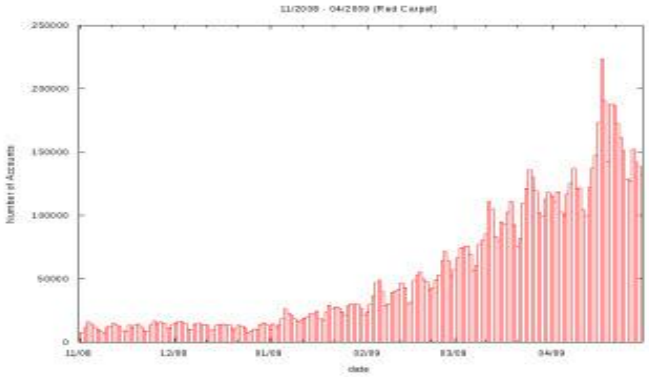
Twitter Growth
Red Carpet Era

Twitter Account Creation 2006-2009

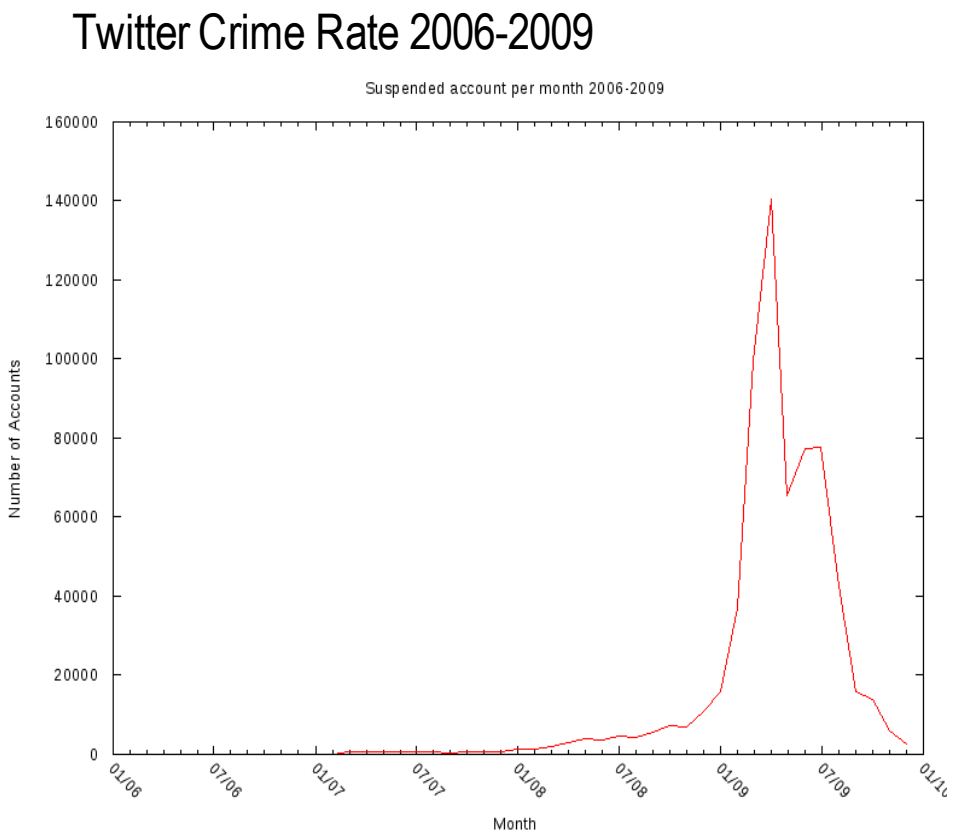


- 54% of the 50 Most popular Twitter users started using Twitter during the Twitter Red Carpet Era.
- Twitter growth rate went from 2.02% in Nov 08 to 21.17% in April 09.

Twitter Account Creation
Red Carpet Era (11/08-04/09)



Twitter Crime Rate
2006-2009



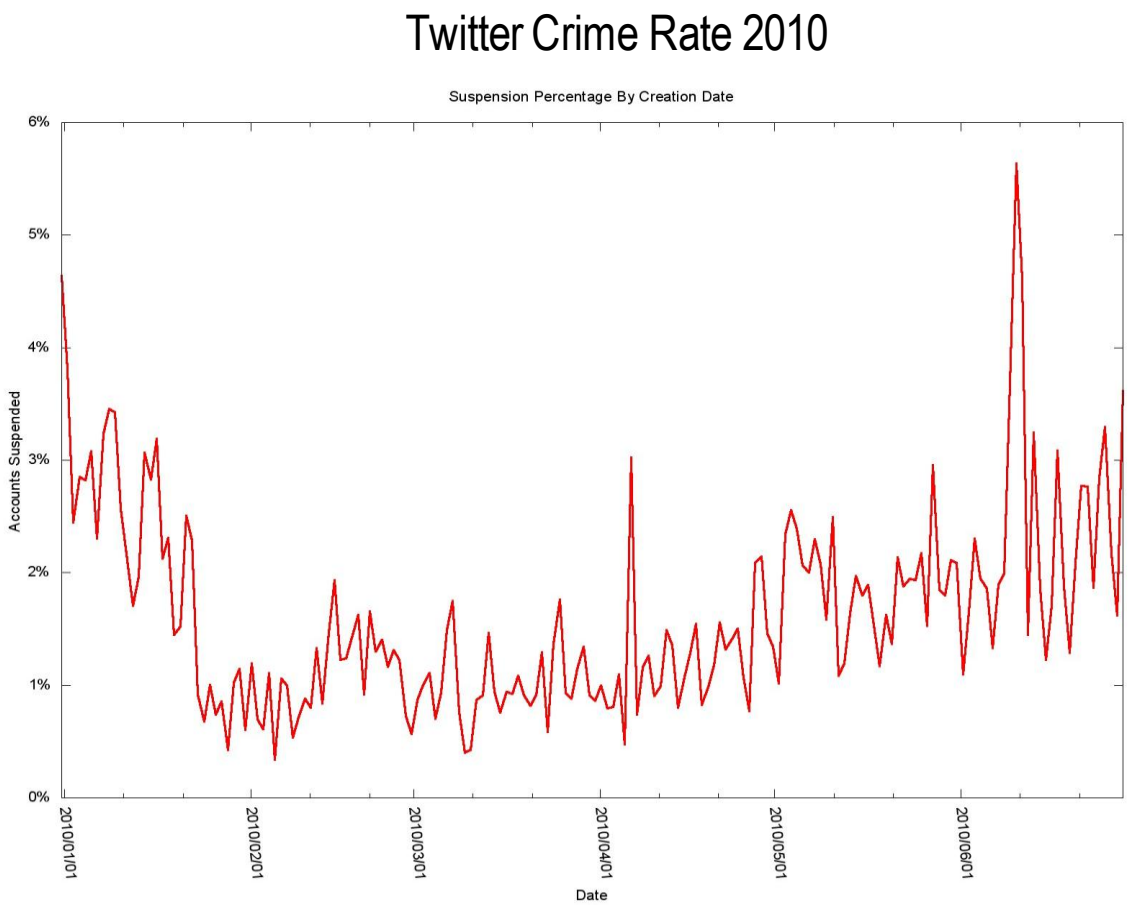
- 2006 = 1.2%
- 2007 = 1.7%
- 2008 = 2.2%

During Red Carpet Era:

- Twitter Crime Rate increased 66% from 2.02% to 3.36%

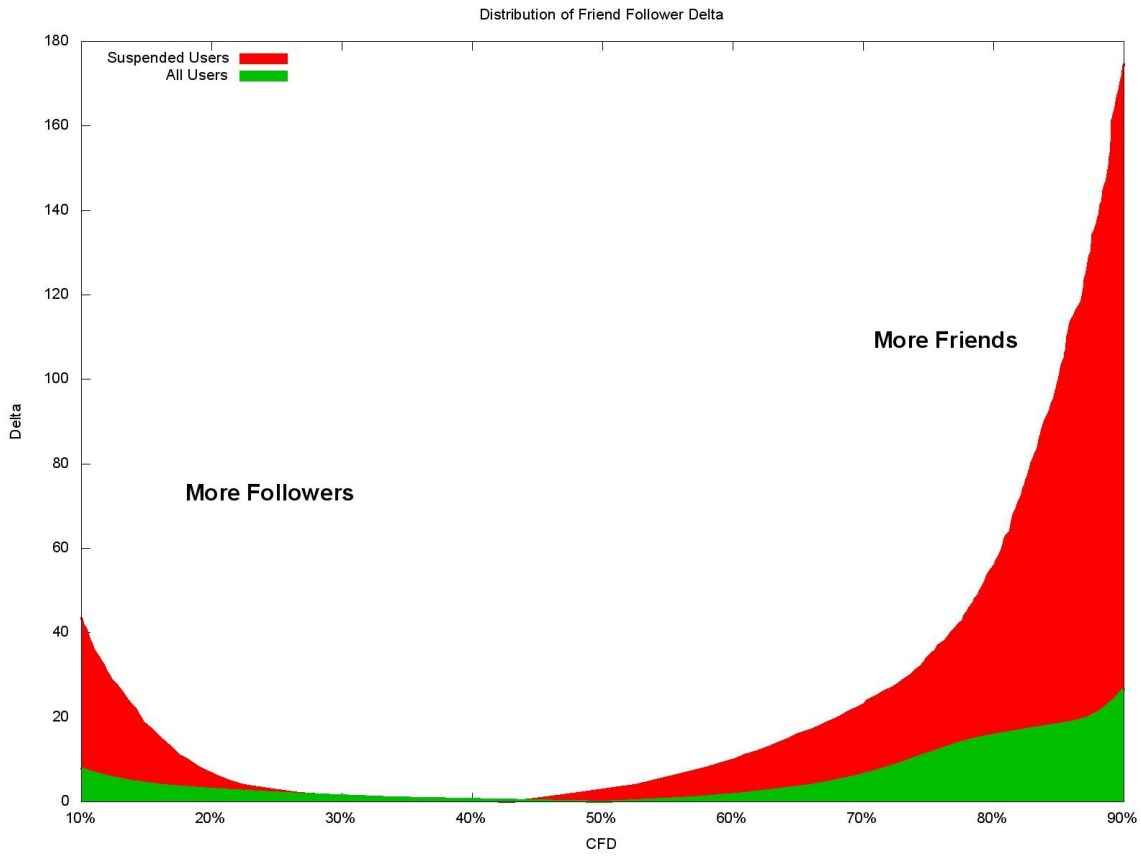
- This more than tripled over the following four months, escalating to 12% in October 2009.

Twitter Crime Rate
2010

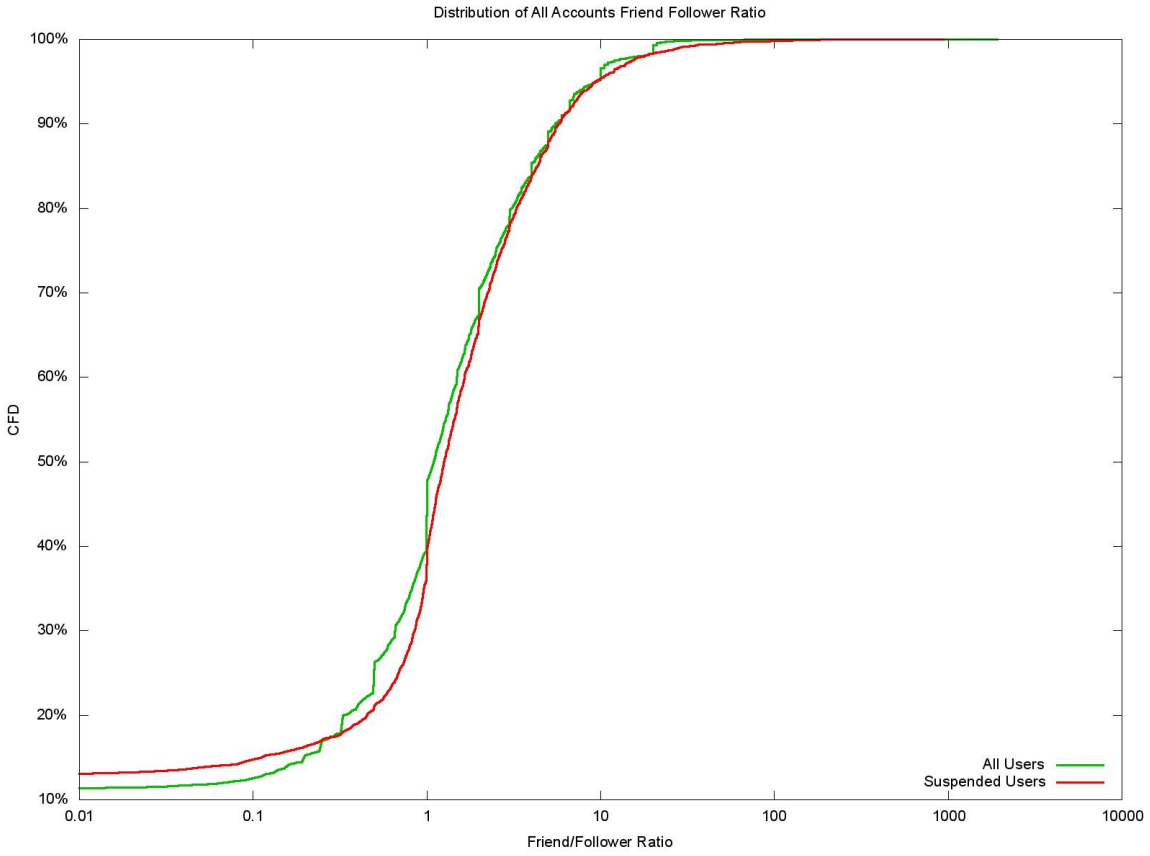


Suspended Accounts
Friend Follower Delta

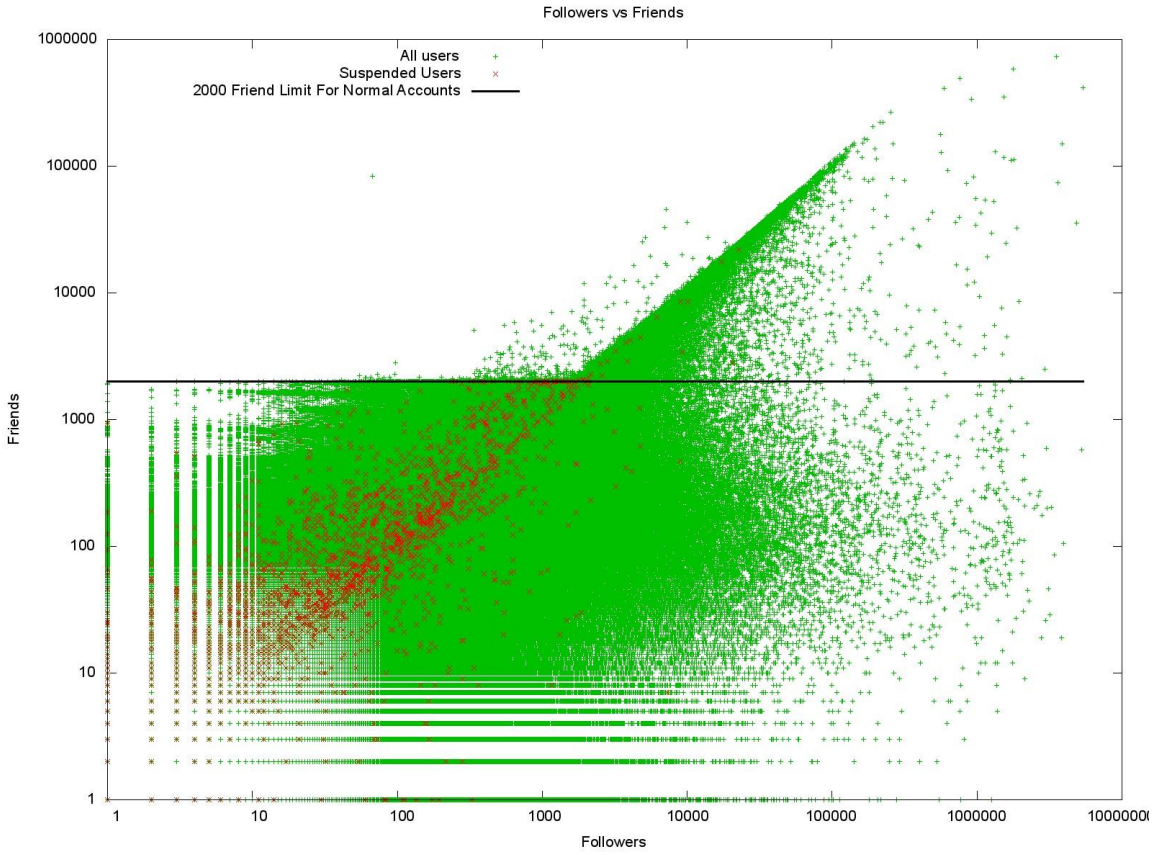
Suspended Accounts Show Greater Delta in Friend/Follower Delta



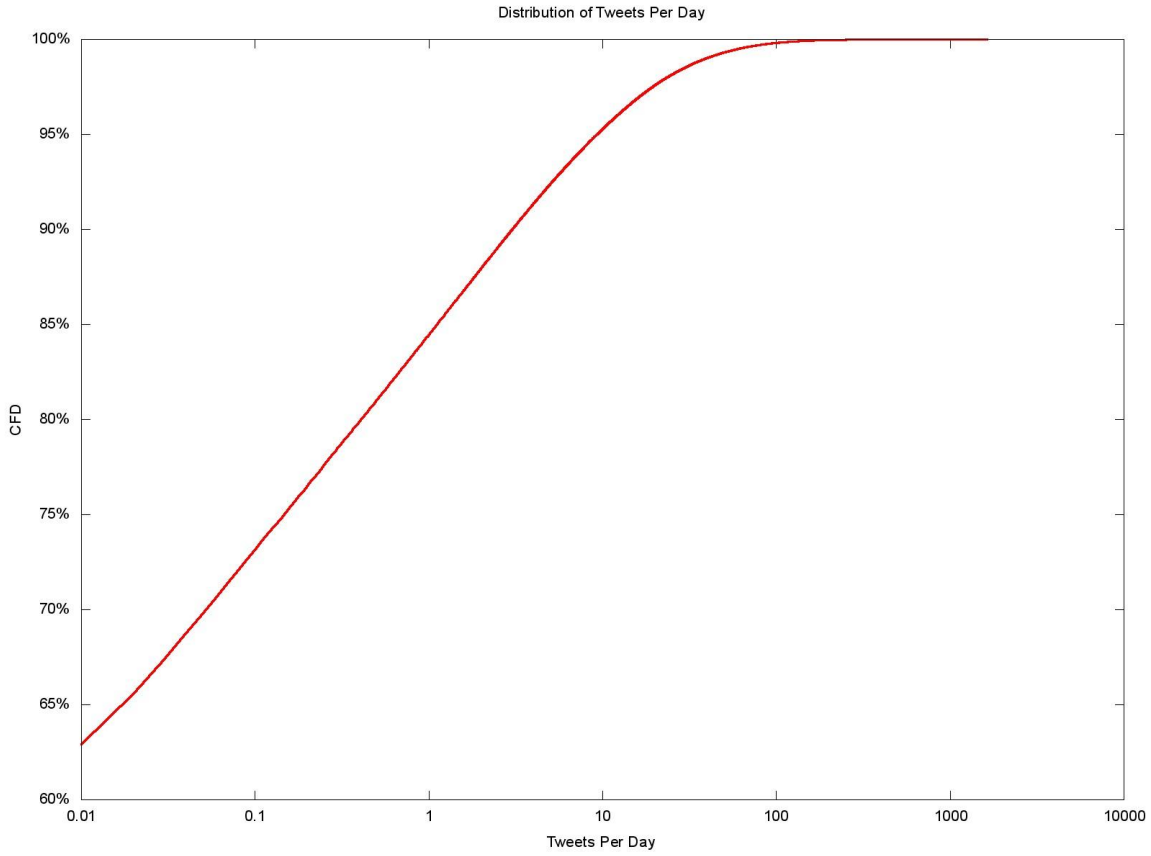
Suspended Users:
Friend Follower Ratio



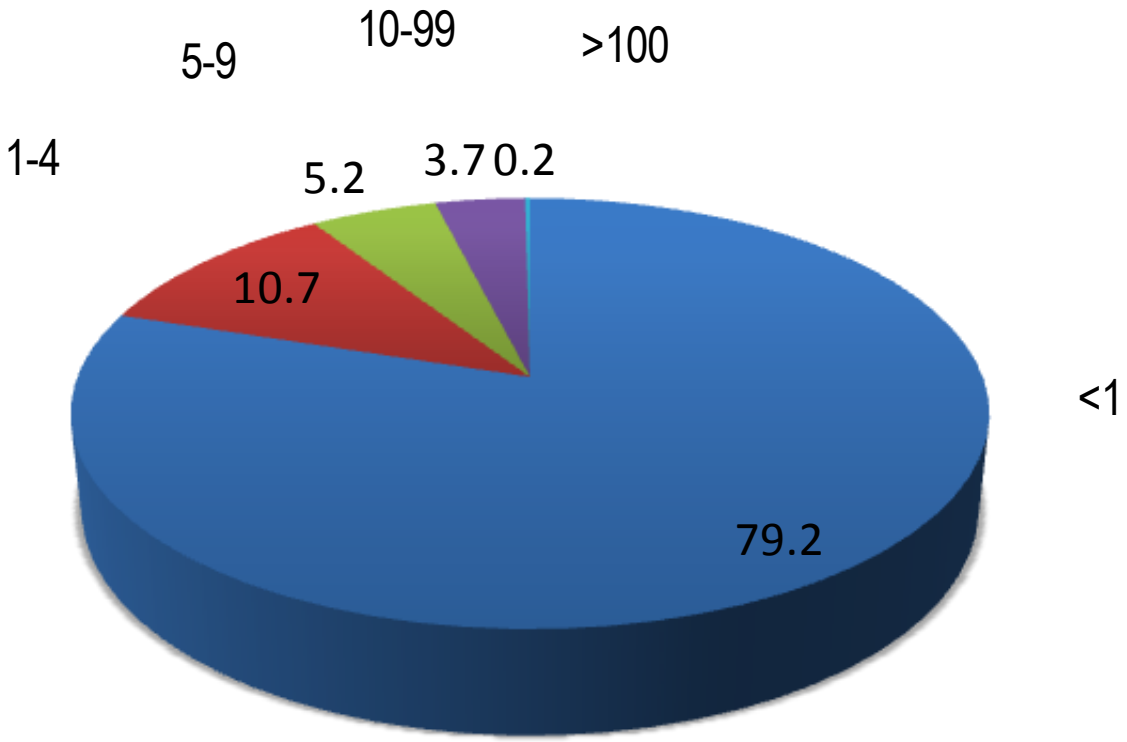
Suspended Users:
Followers vs. Friends



Tweet Number
Average Tweets Per Day

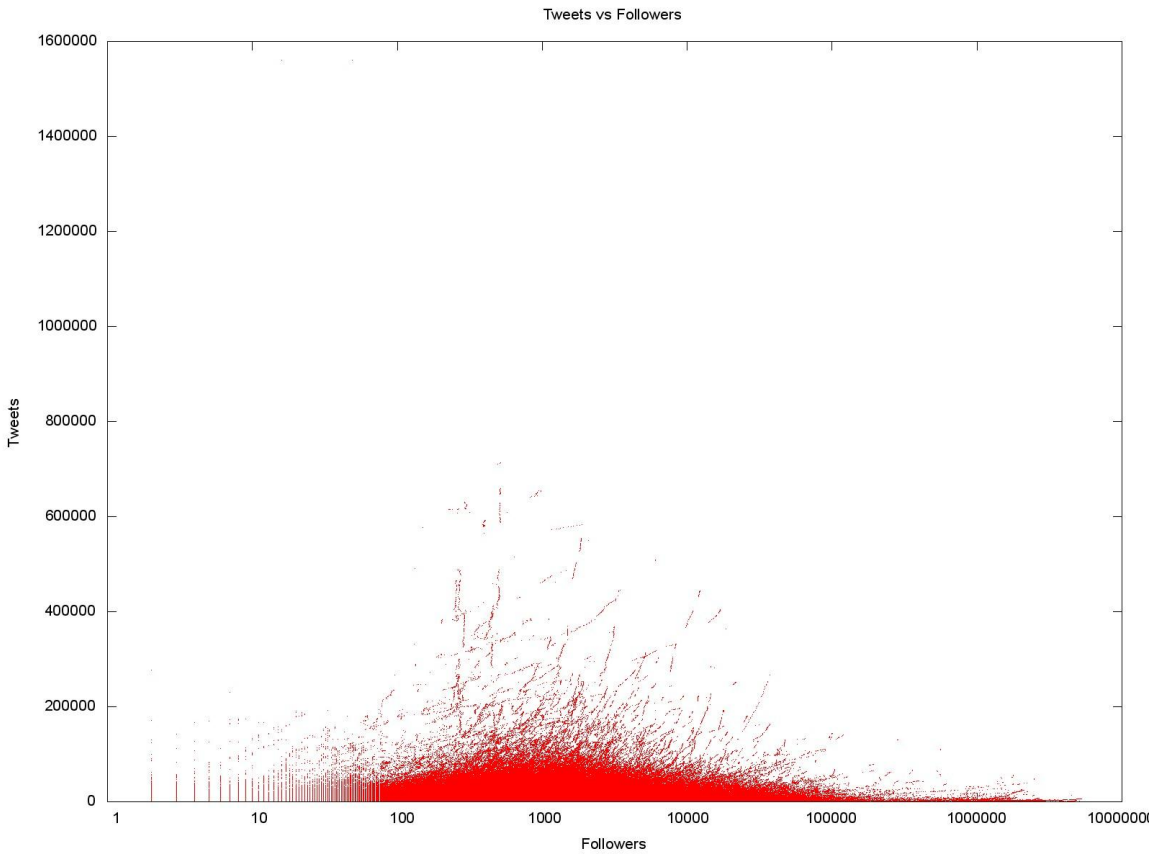


Tweet Number
Average Tweets Per Day



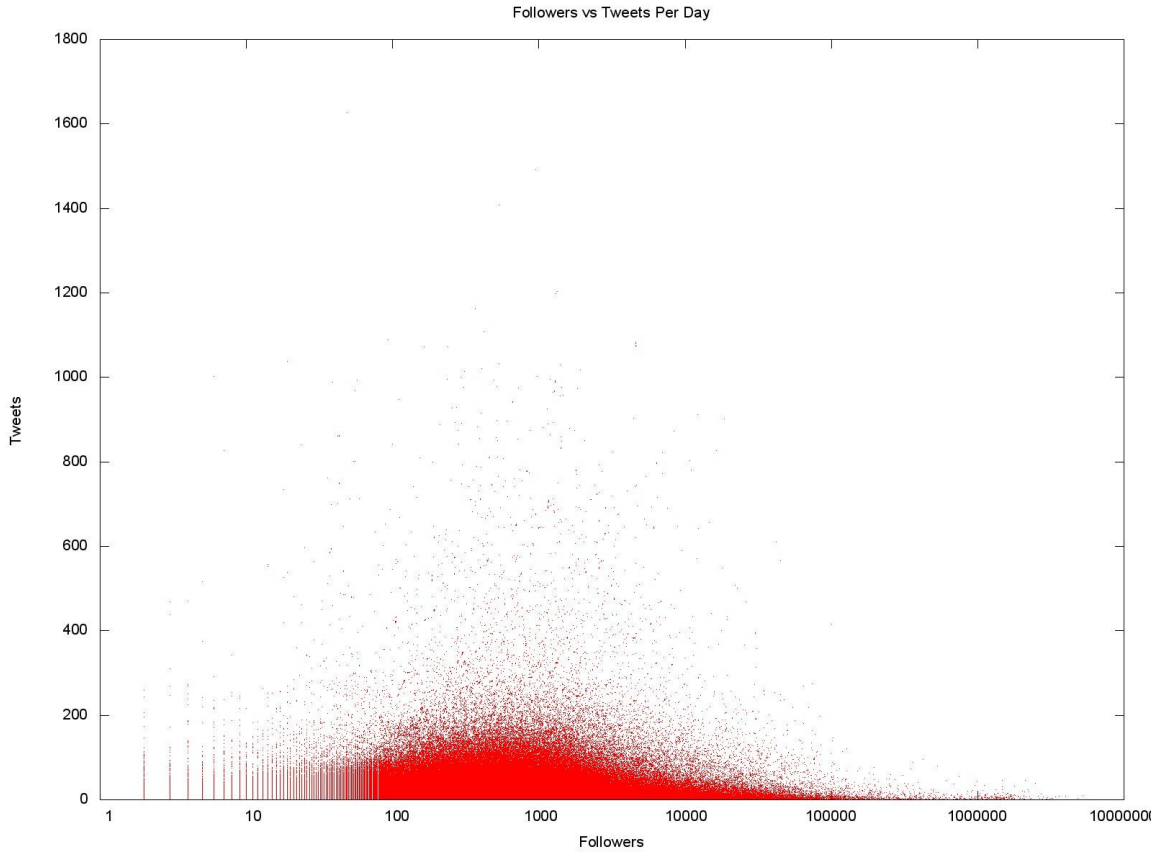
Followers vs. Total Tweets

The Most Active Accounts Are Those With 100-10000 Followers



Followers vs. Tweets Per Day

Very noisy accounts are not able to attract large numbers of followers.



SUMMARY: TWITTER TRENDS & TRACKING

- Legitimate users are using Twitter more.
- However, the majority of Twitter accounts still go unused.
- Behavior-based features show promise of building a foundation for User Reputation.

FACEBOOK

MALICIOUS LINKS & APPS

Facebook Social Attacks

Leverage social/viral component to reach victims

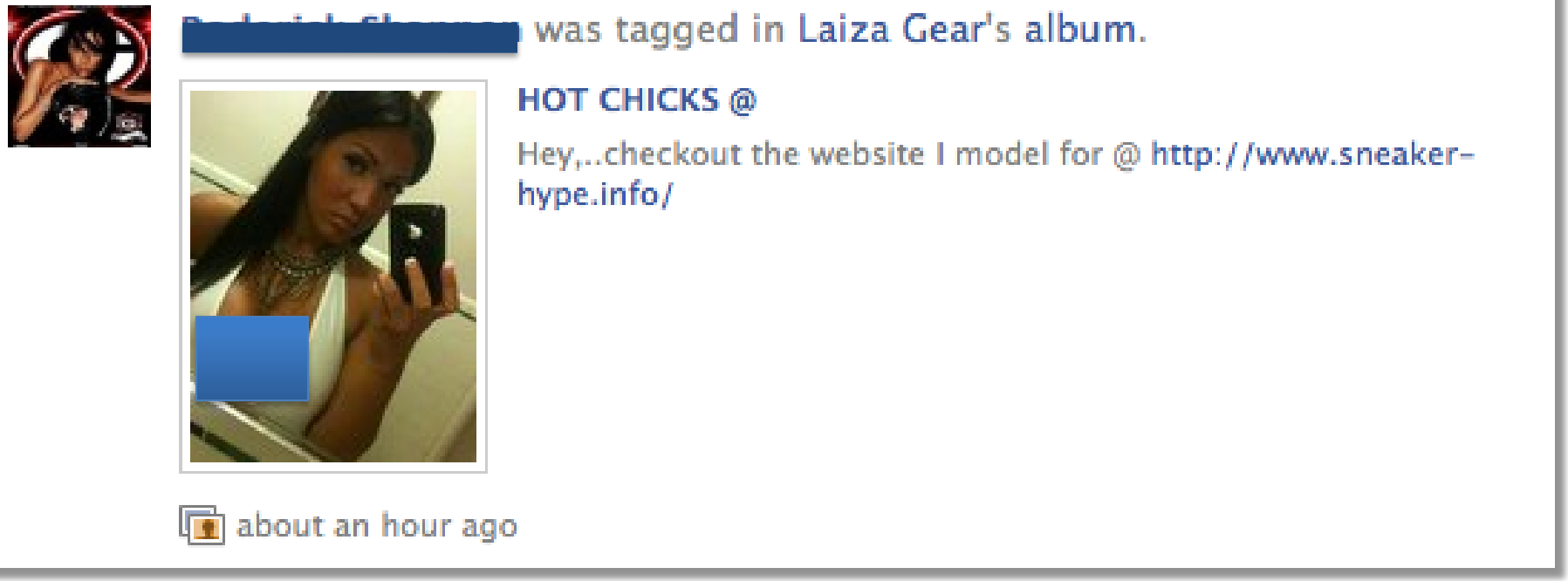


Photo “Tags” up to 50 People

Wide distribution of malicious links

Yeah, a bunch of us model, just visit this site http://www.jordan-home.info/

In this photo: Wilbert Thomas, Terrance Houston, Travis Doubleyou, Vaughn Fontenot, Tobias Tha Kidd Bryant (photos), Ulm Alphas Etachi (photos), Tony Converse, Tiera Shawuan Matthews, Tramelle Howard (photos), Wilbert Bradley, Trevor Olivier (photos), Tyrus Lawson, Thomas Nguyen, Timmy Barral, Tee Wiggler Zeigler, Timothy Smith, Travon Hollis, Travis Lindsey, Taye Scott, Torey Jones, Trell Williams, True Vine C.M., Zil Reddrobotz Barton, Terry Gorrell, Terrell Alexander II (photos), Venell James, Yung Jody (photos), Trezley Lockhart, WayneGretzky Shitting OnHoes, Warren Roberts, Yc Dontforgetmymoney, Wilbert Webb, Tj Tolbird, Travis Carter, Trevonte' Veinticinco Carter, Timothy McCall Jr. (photos), Yung Ceasar Palachie Narcisse (photos), Thaddeus Esteve, UlmQ-dawgs MuLambda, Trevon Ledet (photos), Ulm Sigmas, Willie Ruiz, Ulysses McDaniel, Valan May, Terrance Brown, Young Choppa, Tyshawn Rocafella Clax, William White

Added 42 minutes ago

Travis Lindsey likes this.

From the album:
have fun at http://www.j
home.info by Cherry Ech

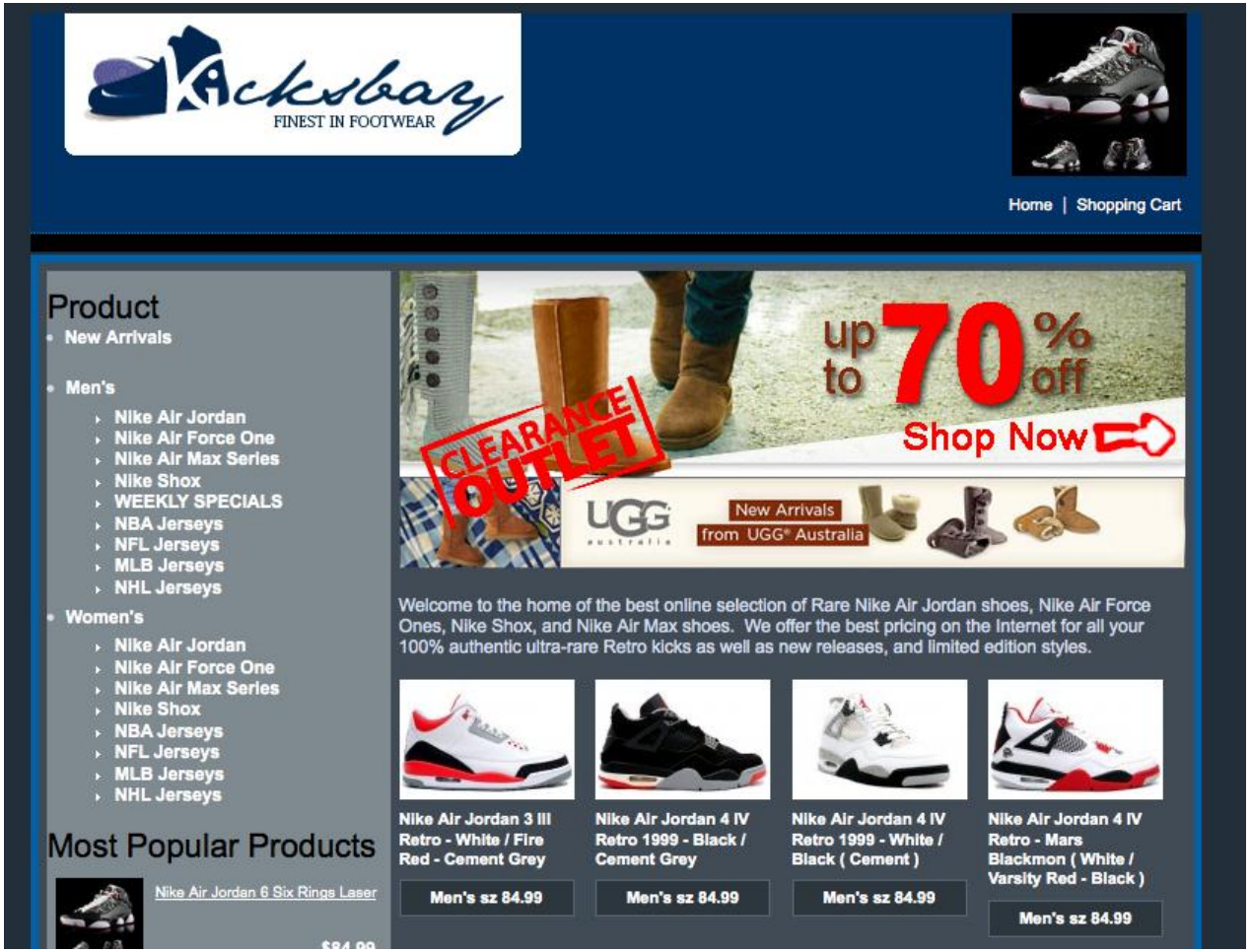
Share

Tag This Photo

Report This Photo

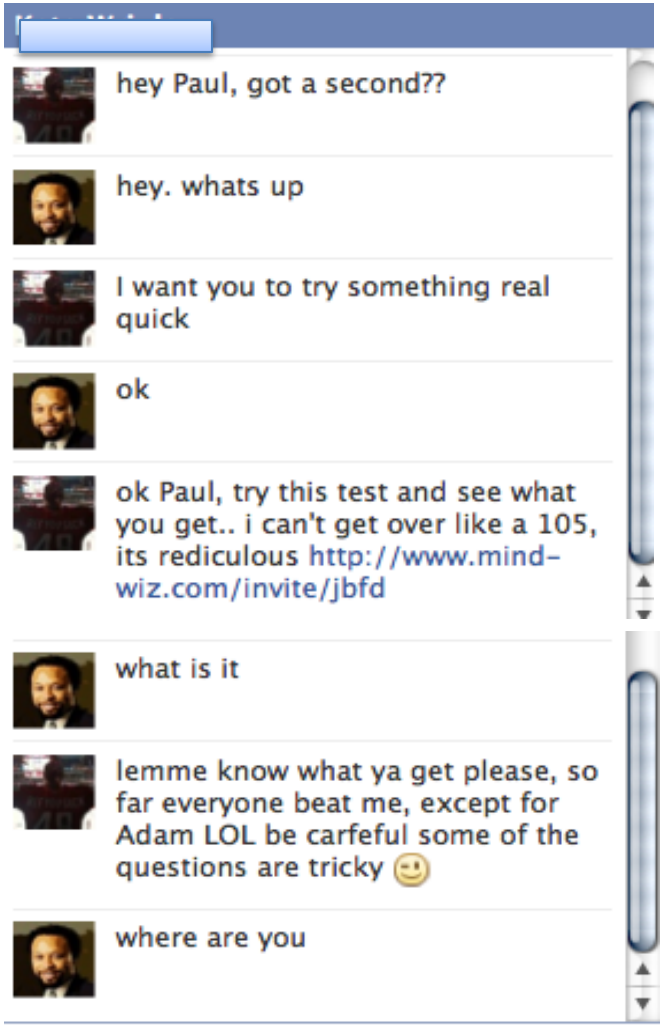
Facebook Advertising

Selling fake illegal shoes

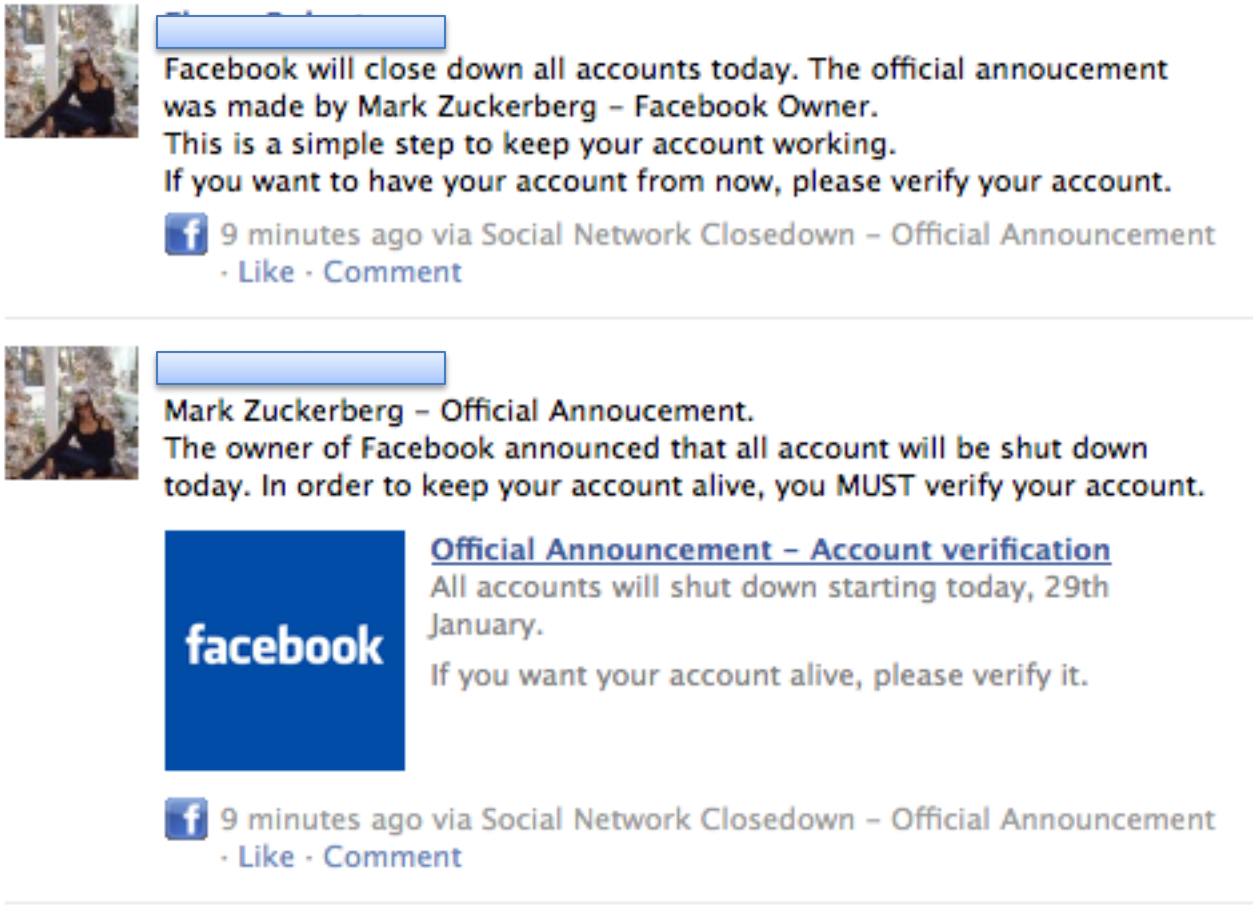


Automated Social Engineering

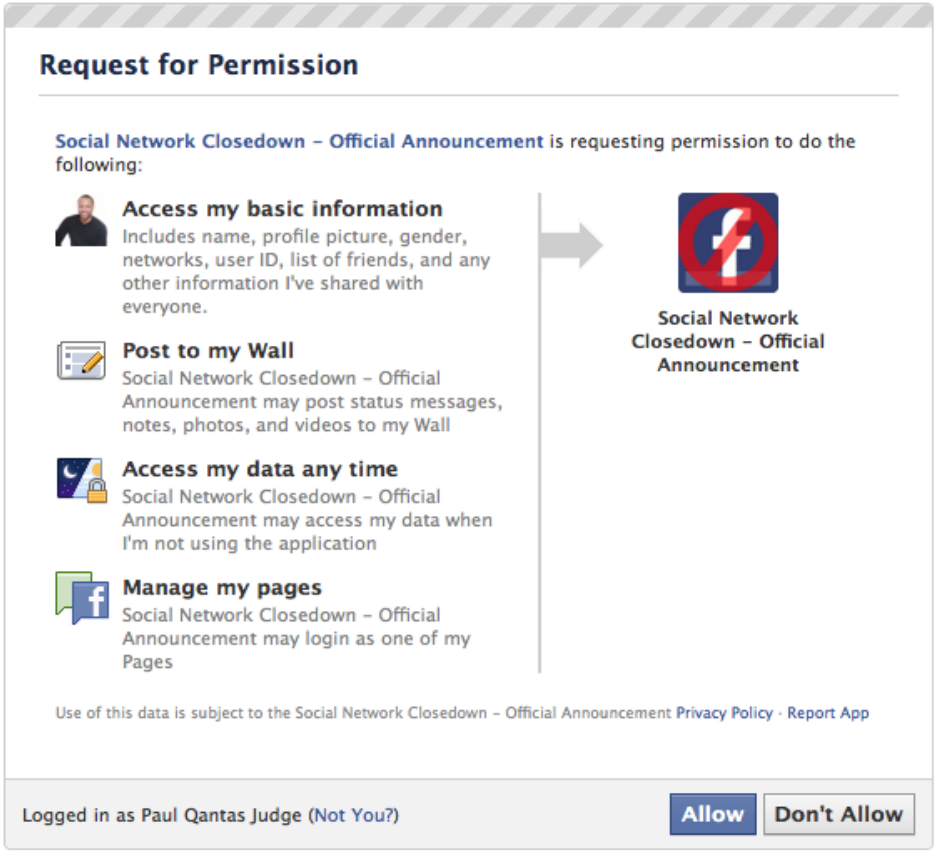
Leveraging Facebook chat



Malicious Facebook Apps



The malicious app requests access to your profile information, list of friends, posting on your wall. It also wants to be able to do this anytime.




WEB APPLICATION SECURITY
SURVEY RESULTS

The State of Web Application Security

Ponemon Institute conducted a study sponsored by Cenzic and Barracuda Networks to determine the state of Web application security. We surveyed 637 IT and IT security practitioners in a variety of industries with an average of 11 years of experience in their profession. The survey focused on the following issues:

- The importance of securing Web-facing applications
- What organizations are doing to augment and secure Web applications
- Perceptions about the use of Web application firewalls (WAFs)
- What organizations are doing to test the vulnerabilities of Web apps

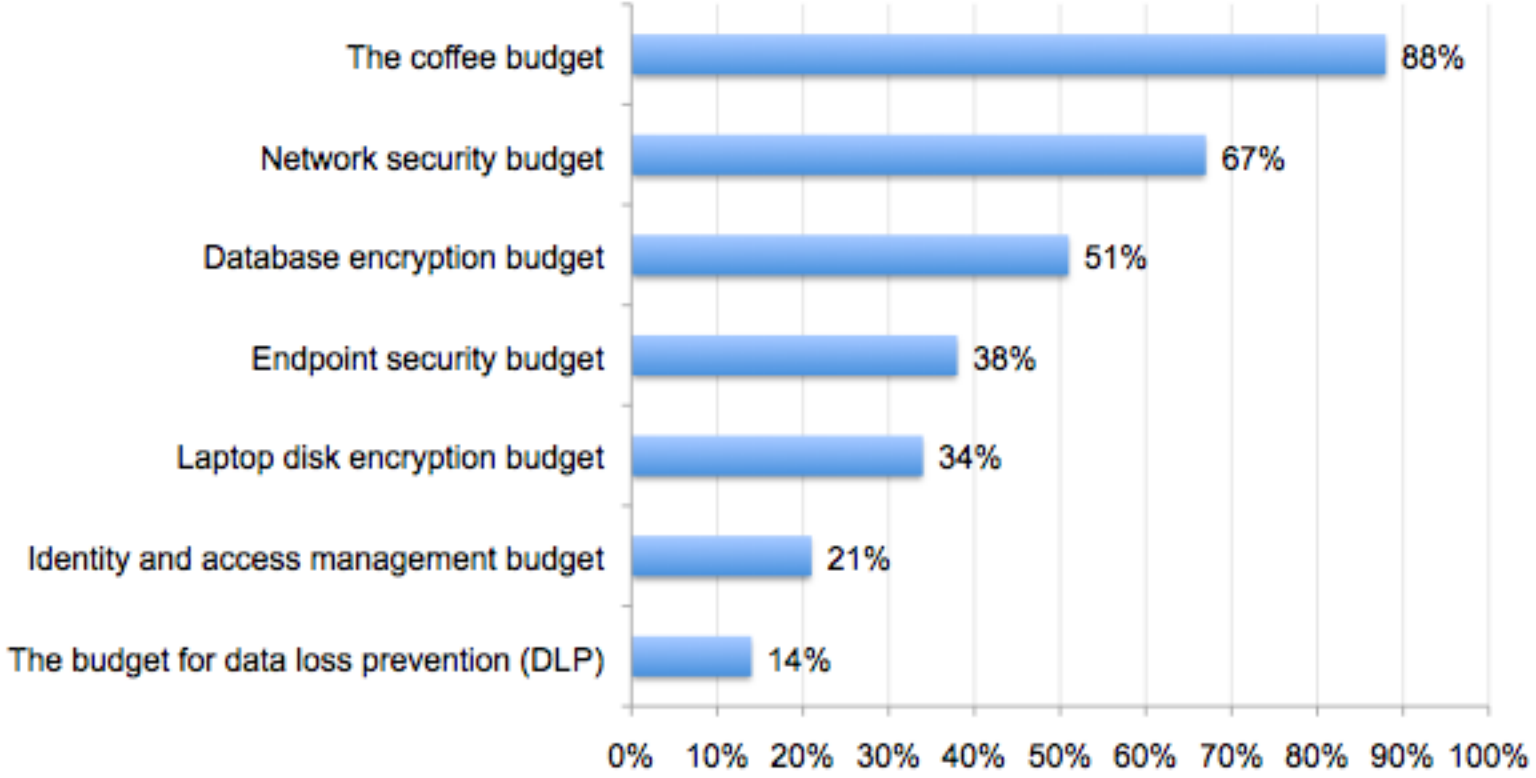
The study reveals the perceptions respondents have about their organizations' experience in protecting Web applications. Seventy-four percent of respondents believe Web app security is either more critical or equally critical to other security issues faced by their organizations. When asked what the economic impact would be if they had a hacker attack, 25 percent say it could be more than $5 million and the average is $255,000. It is clear why hacker attacks to Web apps could be costly because of the potential for the loss of sensitive data, fines due to noncompliance with regulations and business disruption.

What statements best describe your organization's web app security budge relative to other budgeted items?

Ponemon INSTITUTE

Our company's web app security budget is less than . . .

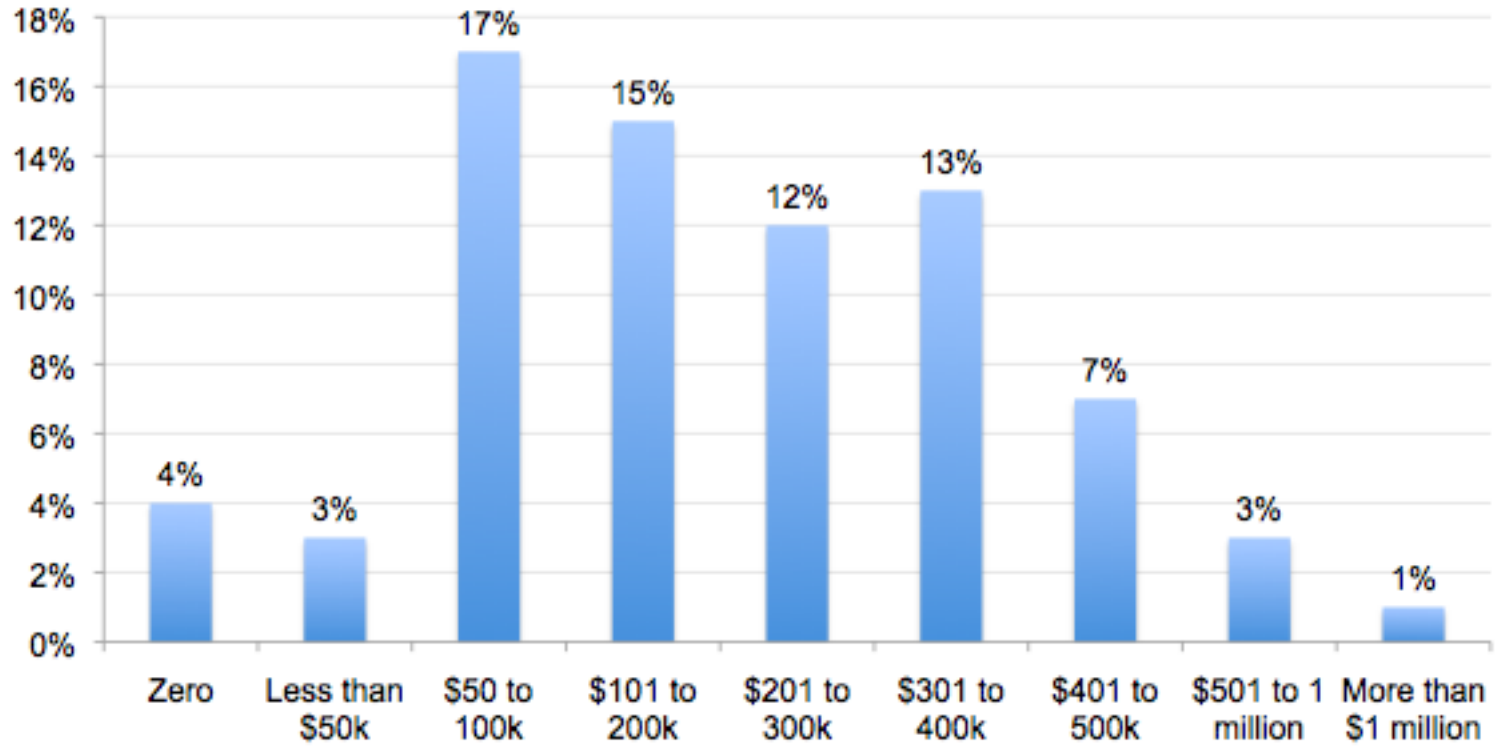
Sample includes 637 IT and IT security respondents



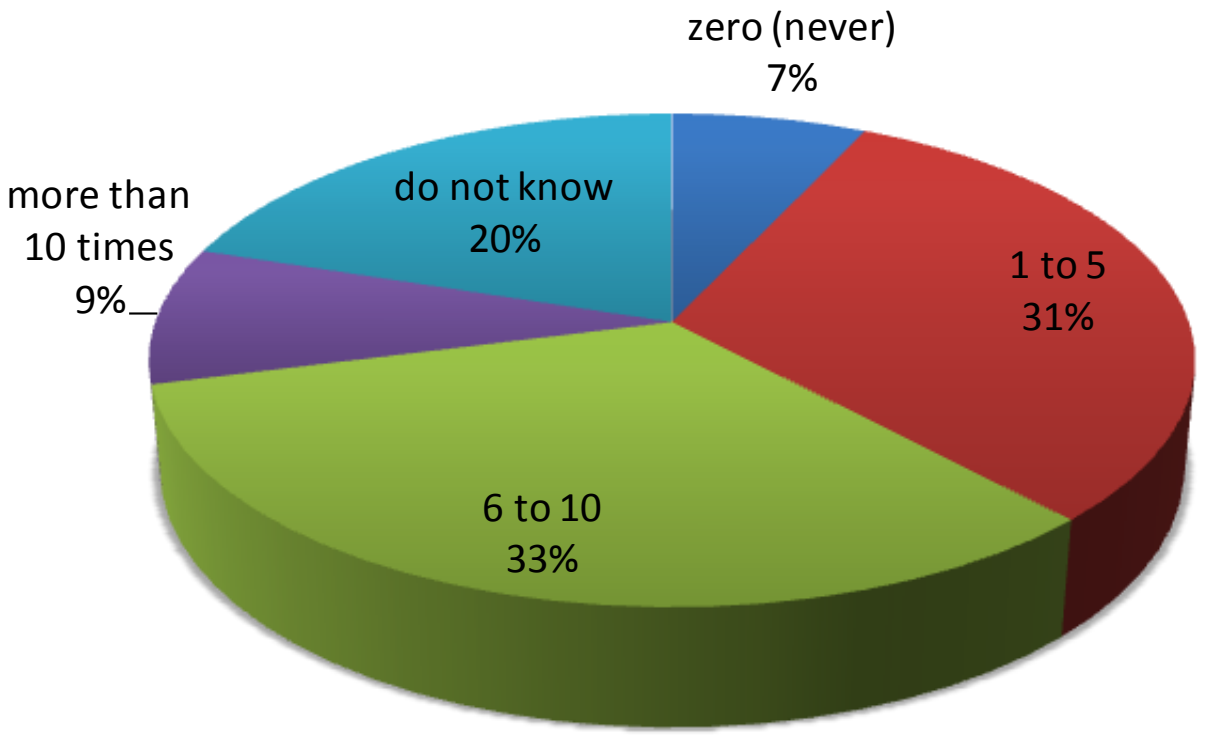
If hacked, what do you think it would cost your organization?

Sample includes 637 IT and IT security respondents

Extrapolated value is $255,000 for the present sample.



73% of companies have been hacked in last 24 months



ACKNOWLEDGMENTS

This report represents some examples of the work performed in 2010 by Barracuda Networks in protecting our more than 130,000 customers. This includes the efforts of our engineering, support and research teams in the Americas, Europe and Asia. We would like to acknowledge our customers for trusting us with the responsibility of keeping their users and networks safe. We also would like to acknowledge our data sharing partners and research affiliates.

For ongoing updates, please visit BarracudaLabs.com and follow @BarracudaLabs on Twitter.

www.BarracudaLabs.com

BARRACUDA LABS

2010 ANNUAL SECURITY REPORT

BARRACUDALABS