Following the tracks
Understanding snowshoe spam

Image source: wikipedia.org
War on spam…

- Decline of “botnet” driven spam over the past 12 months
CAN-SPAM Act of 2003

- Functional unsubscribe
- Postal address
- No forged headers
- No sending to harvested addresses
- Send via your own network
Spammer’s Dilemma

CANSAMP Compliance
Sustainable Deliverability
CANSPAM REQUIREMENTS

• Functional unsubscribe
• Postal address
• No forged headers
• Send via your own network

COMPLIANCE?

• Yes (mostly), but most recipients do not bother
• Use postal drop boxes to remain anonymous
• Register hundreds or thousands of “throw away” domains
• Lease hundreds of IP addresses from ISPs/Colo/VPS/Cloud
Daily distribution by CIDR

“Limited Trial of the Revolutionary High-Tech Prado Electronic Cigarette!”

<table>
<thead>
<tr>
<th>CIDR / DATE</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>204.8.217.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173.234.147.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>213.175.201.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>208.83.235.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>206.212.252.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38.102.228.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65.49.36..0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69.65.41.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96.8.119.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>213.175.207.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.115.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66.79.182.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>205.209.155.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>208.77.44.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.121.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.123.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.124.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173.134.185.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>184.82.158.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.117.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173.234.185.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96.45.110.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173.212.199.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173.213.61.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.162.113.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Snowshoes!
A closer look...
Sending Behavior

- Statically allocated, dedicated IP addresses
- Paid for by the spammers
- Typically hosted in North America
## Top ISPs abused

<table>
<thead>
<tr>
<th>ISP</th>
<th>Message count</th>
<th>Unique IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>3dgwebhosting.com</td>
<td>799490</td>
<td>16570</td>
</tr>
<tr>
<td>SingleHop</td>
<td>136408</td>
<td>2549</td>
</tr>
<tr>
<td>SoftLayer Technologies</td>
<td>106041</td>
<td>1125</td>
</tr>
<tr>
<td>Limestone Networks</td>
<td>64787</td>
<td>1119</td>
</tr>
<tr>
<td>AccelerateBiz</td>
<td>17457</td>
<td>714</td>
</tr>
<tr>
<td>Nobis Technology Group, LLC</td>
<td>55193</td>
<td>697</td>
</tr>
<tr>
<td>Network Operations Center</td>
<td>53988</td>
<td>691</td>
</tr>
<tr>
<td>FDCservers.net</td>
<td>20460</td>
<td>507</td>
</tr>
<tr>
<td>GigeNET</td>
<td>22913</td>
<td>459</td>
</tr>
<tr>
<td>Global Net Access, LLC</td>
<td>35996</td>
<td>422</td>
</tr>
<tr>
<td>FortressITX</td>
<td>16553</td>
<td>398</td>
</tr>
<tr>
<td>LogicWeb</td>
<td>21685</td>
<td>390</td>
</tr>
<tr>
<td>Colostore.com</td>
<td>22069</td>
<td>378</td>
</tr>
<tr>
<td>iWeb Technologies</td>
<td>65480</td>
<td>306</td>
</tr>
</tbody>
</table>
Financial motivation

- Money is made via a vast array of affiliate programs
- Spammer is the affiliate (publisher)
- Paid via “Cost per Click” or “Cost per Action”
Snowshoe vs “criminal spam”

- Header content

received: from 789.pizzaperu.com (HELO 789.pizzaperu.com) [65.60.47.236]
  by <trap>; <date>
From: "Hybrid Car" <info@pizzaperu.com>
Subject: Go Green Save Green

received: from duper.varichurm.com (HELO duper.varichurm.com) [64.187.106.21]
  by <trap>; <date>
Subject: As A Homeowner This Product Saved Me Thousands
From: "Surface_Seamers" <sealsurfaces@varichurm.com>
Snowshoe vs “criminal spam”

• Header content
• Unsubscribe link and contact address
Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”
Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”
- Targeted recipients
Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”
- Targeted recipients
- Products advertised
VS Solicited bulk email

- Similar visible content
VS Solicited bulk email

- Similar visible content
- Spam content found in the body

```html
<style type="text/css">
    ring breaks at last nights gig. Shop says tama won't replace under warranty and tama won't talk to me.

    For the money these are I'm not impressed. Anyone else had similar?
    Reply With Quote
    #2
    Old 07-06-2011, 12:56 PM
    uniin's Avatar
    uniin uniin is offline
    Silver Member

    Join Date: Sep 2010
    Location: Blue Mountains, Australia
    Posts: 609
    Default Re: New iron cobras = useless tama....
    are you putting max tension on your springs, and burying the beater into your bass drum (thus creating a lot more tension on your spring)?
    [snip]
</style>
```
VS Solicited bulk email

- Similar visible content
- Spam content found in the body
- Domains used
VS Solicited bulk email

- Similar visible content
- Spam content found in the body
- Domains used
- Source and history of IPs used
What makes it a problem

• Volume varies wildly
What makes it a problem

- Volume varies wildly
- Unsubscribing may not work
What makes it a problem

- Volume varies wildly
- Unsubscribing may not work
- Lack of action response and action by ISPs
What can be done?

• Legislation based on consent (like FISA)

• ISPs must review and take action on abuse complaints

• More coordinated monitoring and abuse reporting

• Draw more attention to the problem
In conclusion

- It’s a growing problem for many people
- It’s still a spam (unsolicited bulk e-mail)
- It’s very different from a criminal spam
- We need to raise awareness and take action
Questions?