Abuse and the Global Infection Rate

August 2006
DEFCON-14
Rick Wesson
CEO, Support Intelligence, LLC
Problem Statement

- It is hard to know when a device on your network has become owned or compromised.
- The number of compromised systems grows daily by Millions of nodes per day.
- how do you unfuck this?
Defining Abuse

• Sending [lots of] SPAM/UCE
• Hosting open proxies
• DDoS
• Botnet C&C
Identifying Abuse

- BlackLists
- DNS
- Honey pots
- Spam Traps
- Botnet Sinkholes
woody-maclen

economic theory of abuse

Overlap

Revenue '06

Revenue Derived from SPAM/Click Fraud

Cost to deploy a botnet

Costs '06

Incentive
Gap

Revenue '09

Revenue Derived from SPAM/Click Fraud

Cost to deploy a botnet

Costs '09

Incentive
Visualizing Event Data

- Realtime Abuse Data
- BotViz tool
- Apparently useless but fun
Annotomy

- Controller Capabilities
- Socks Proxy
- Web Frontend
- Commands and Management
- Drop File Analysis
  - who, what and where
  - what got compromised
Controller View

Remark: displayed only online socks (socks that were in online in last 20 minutes)
Remark: to copy IP or ID to clipboard press button "copy IP" or "copy ID"

Select by country: All countries
Select by state: all

Current country selected: all
Current state selected: all

<table>
<thead>
<tr>
<th>IP</th>
<th>SOCKS</th>
<th>ID</th>
<th>COUNTRY</th>
<th>CITY</th>
<th>STATE</th>
<th>CONNECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>81.215.219.6</td>
<td>39221</td>
<td>LCEYTVPAMTTSVPNWZSNIVHHWCRVCLV</td>
<td>Turkey</td>
<td>Türk</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>200.11.0.70</td>
<td>15969</td>
<td>NXXCGTQVFPRPGVZSIXZPJRHYHTLDC</td>
<td>Brazil</td>
<td>Seropédica</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>172.158.42.134</td>
<td>53482</td>
<td>AGEFCXLKBESMVIPQXVOQSOOSTYJEVD</td>
<td>United States</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>86.51.0.134</td>
<td>20989</td>
<td>FCSUZZTCJTDHIUSXSMQAZWUPCT</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>67.187.128.155</td>
<td>30438</td>
<td>UAYOGLCBDTTNCDFDPZOHJMNHHLVCF</td>
<td>United States</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>204.111.231.232</td>
<td>22352</td>
<td>FEPRVBMTVIPSXWENUGPGLFYNBXIIYH</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>66.61.139.21</td>
<td>25195</td>
<td>HHZMMEIZCNYARXDFXHTECFPGCJPIQA</td>
<td>United States</td>
<td>Herndon</td>
<td>VA</td>
<td>1</td>
</tr>
</tbody>
</table>
### SOCKS Proxy

<table>
<thead>
<tr>
<th>Copy IP</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
<th>Copy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>65.27.228.229</td>
<td>28420</td>
<td>LIQSXPNWBJPELDYKEHHBGFMUABWQ</td>
<td>United States</td>
<td>Herndon</td>
<td>VA</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>84.9.24.22</td>
<td>28372</td>
<td>BSYUOMQEPSERBFTBNHCKSHJUWKA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67.187.78.37</td>
<td>45056</td>
<td>GPETNFNMBXQKKNRUXPHALVNLNXZPAF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>213.224.85.28</td>
<td>33482</td>
<td>RIAQGNEWYICRMWDJHAYRBNWBYGGAHV</td>
<td>Belgium</td>
<td>Mechelen</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>142.169.28.203</td>
<td>16398</td>
<td>XWOJVCOXDUEAHMXENAYWFDOWYPQF</td>
<td>Canada</td>
<td>Rimouski</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>67.139.110.187</td>
<td>45208</td>
<td>XVFSIKYVZCMIFQASWOSBNCPXRZBNFS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72.152.153.159</td>
<td>58441</td>
<td>TXOCYLDDEFXHLSPLJQPBLYEHJQAQMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69.140.19.111</td>
<td>54119</td>
<td>HWBCDKHMXORUGJVARROZVWGVXJDZGL</td>
<td>United States</td>
<td>Cherry Hill</td>
<td>NJ</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.146.78.235</td>
<td>36952</td>
<td>AYTBJXZDJRRKDAEWTWIKKYYCCJH</td>
<td>United States</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.43.223.58</td>
<td>45927</td>
<td>XCOKPPADICSGWLEACGAXZSOYWEPAFYR</td>
<td>United States</td>
<td>Parsippany</td>
<td>NJ</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.121.28.6</td>
<td>47267</td>
<td>ELVWSSVXSBQDTLJFIGPEZVAMJRCSBD</td>
<td>United States</td>
<td>Princeton</td>
<td>NJ</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>84.62.178.142</td>
<td>54719</td>
<td>RNMTATQODHMZQUMLWPLJULKWEHMR</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.44.60.71</td>
<td>35978</td>
<td>EMMENHHUBVBPRKPHOTISLNBAPVVSJ</td>
<td>United States</td>
<td>Stamford</td>
<td>CT</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70.39.34.55</td>
<td>39559</td>
<td>LIFDLZSAQITESLDPNAIPKXGESXWSMT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Other Capabilities

<table>
<thead>
<tr>
<th>Function</th>
<th>URL</th>
<th>Local Filename</th>
<th>Personal Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download and Exec File</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Shell Command</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Store Screenshot in Local File</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Change URL for Logs</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>URL That Should Be Blocked</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Clear Hosts File</td>
<td>[Input]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Upload File</td>
<td>[FTP]</td>
<td>[Input]</td>
<td>[Input]</td>
</tr>
<tr>
<td>Upload Hosts File</td>
<td>[Input]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Remark: in "SHELL COMMAND" do not use symbol ":", bots checks the next command each 5 seconds. Send next command after this time is left.*

[Submit]
Analysis of Data Gathered

- 793 uniquely compromised systems
- 17,195 data captures over 30 days
- 35,867 form logs (multiple per data capture)
- 100% MS Windows XP IE 6.0.2XX
Data Captured

- remote address, time stamp, system information
- captured passwords for pop, imap, telnet
- https posts, http{s} form data
- File regex results (email addresses, ssn, address book contents, urls with login info)
Effected Companies

- ea aol msn craigslist passport ebay
- overstock postbank chase paypal zionsbank
- virgin target yahoo wells fargo verison t-mobile ml vangard fiedlity postini navyfcu
- capitolone wachovia wamu speedpay ebay
- paytax.nat.gov.tw citybank americanexpress sprintpcs usbank esurance wallmart
- ticketweb us.army.mil
Compromised Information

- 54,926 login credentials / clear-text passwords
- 281 unique credit card numbers with address and ccv
- 2,158 unique email addresses of your friends [gathered from your address book]
- 299 Identities (name, address, phone number)
- better parsers could yield 4X more info, I didn’t analyze url encoded data
Account Value

- 1,239 businesses effected (many in the US)
- 35 Brokerage
- XX Bank Accounts
- 86 Bank Accounts
- 174 e-commerce Accounts
- 863 Porn Accounts
- 245 E-Mail Accounts
What is it worth?

- Identities with brokerage with balance < 3K $40 each >= 3K for $70 each. 35 accounts estimated worth $2,450 income for the “bad guy”
Trends and Statistics

- Reviewed 101 Million events over 6 months
- 48M unique ipv4 address
- Spans 12,452 of 19,000 ASN
- Average rate of 267,489 new infections per day.
Routed Autonomous Systems

- Healthy: 55.2%
- Infected: 44.8%
Top 15 Countries with the Most Compromised Systems (1st Half 2006)

- China: 8,917,862 (25%)
- USA: 2,703,990 (8%)
- Korea: 2,137,954 (6%)
- Germany: 2,076,499 (6%)
- France: 1,825,159 (5%)
- Spain: 1,073,024 (3%)
- Brazil: 1,330,111 (4%)
- Japan: 1,029,265 (3%)
- Taiwan: 888,911 (3%)
- Poland: 856,496 (2%)
- India: 543,823 (2%)
- Italy: 319,858 (1%)
- United Kingdom: 510,083 (1%)
- Other 118 Countries: 4,940,107 (14%)
- EU: 4,903,317 (14%)

Colors for countries:
- China
- EU
- USA
- Korea
- Germany
- France
- Spain
- Brazil
- India
- United Kingdom
- Italy
- Other 118 Countries
Chinanet Backbone 221.220.192.0/18

# new IP

Date

4/15/06  4/22/06  4/29/06  5/6/06  5/13/06  5/20/06  5/27/06  6/3/06  6/10/06  6/17/06  6/24/06  7/1/06

Series1
Tools

- REACTb [http://support-intelligence.com](http://support-intelligence.com)
- Micro Soft SNM
- Yahoo!
Gratis

- Yahoo, MicroSoft
- Spamaus, SORBS, SURBL, URIBL, et. al.
- BGP: ISC (vixie) PCH (woody)
- OpenDNS (hardware, disks)
- FriendsNet (we owe alot-a-favors)