# 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 0wned or compromised.
- The number of compromised systems grows daily by Millions of nodes per day.
- how do you unfuck this?

# Defining Abuse

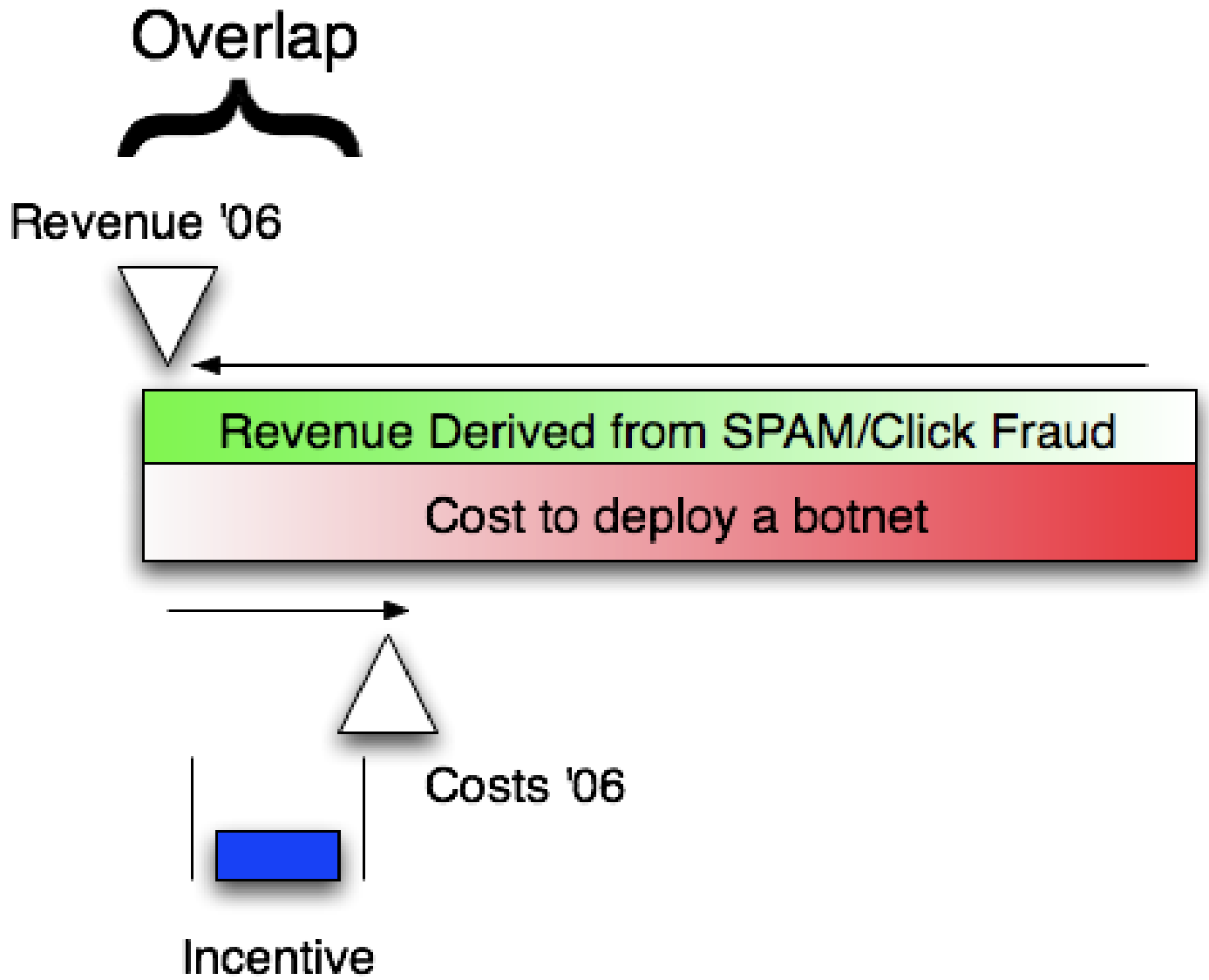
- Sending [lots of] SPAM/UCE
- Hosting open proxies
- DDoS
- Botnet C&C

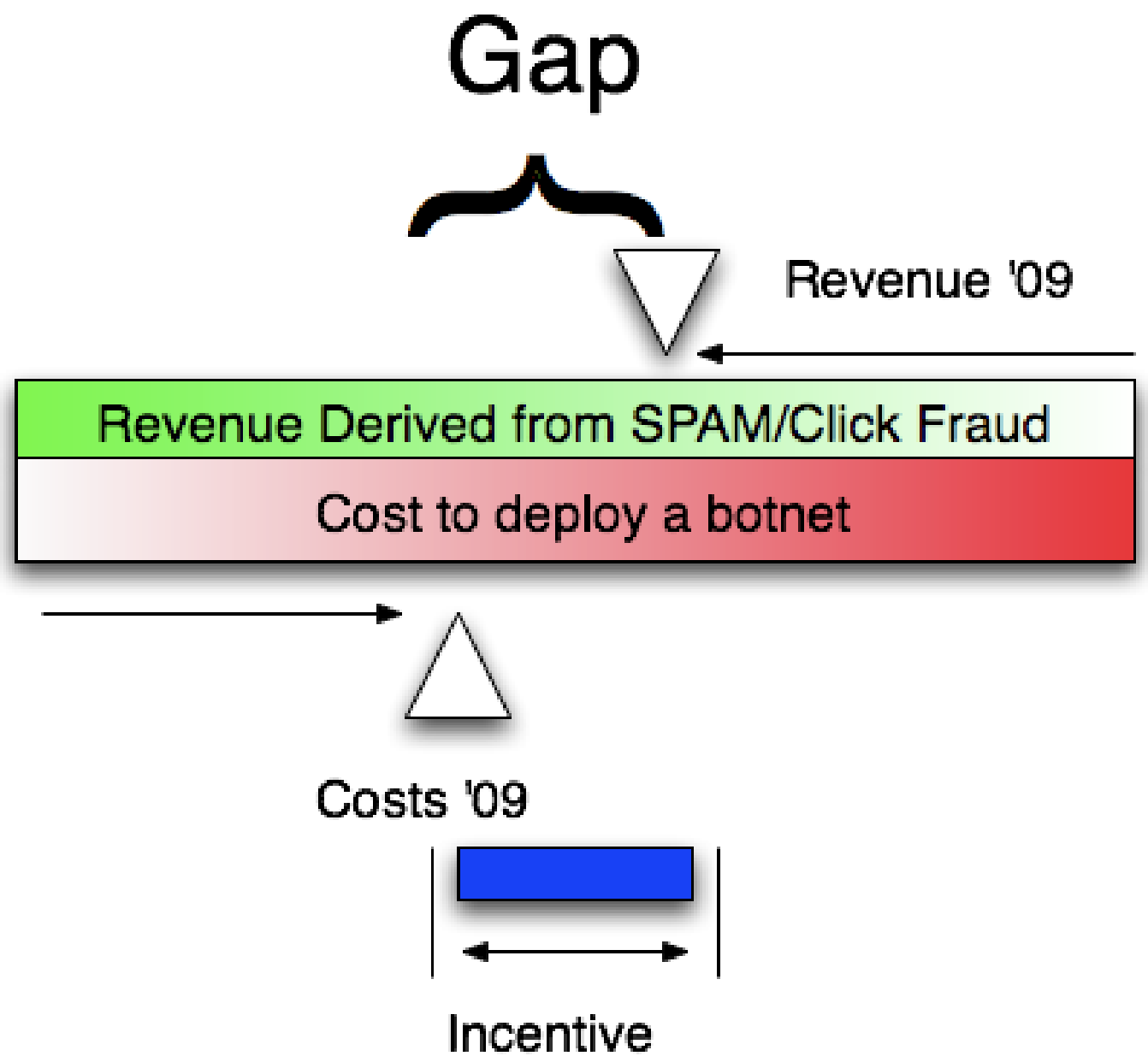
# Identifying Abuse

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

# woody-maclen

# economic theory of abuse




Gap
Revenue '09
Revenue Derived from SPAM/Click Fraud
Cost to deploy a botnet
Costs '09
Incentive

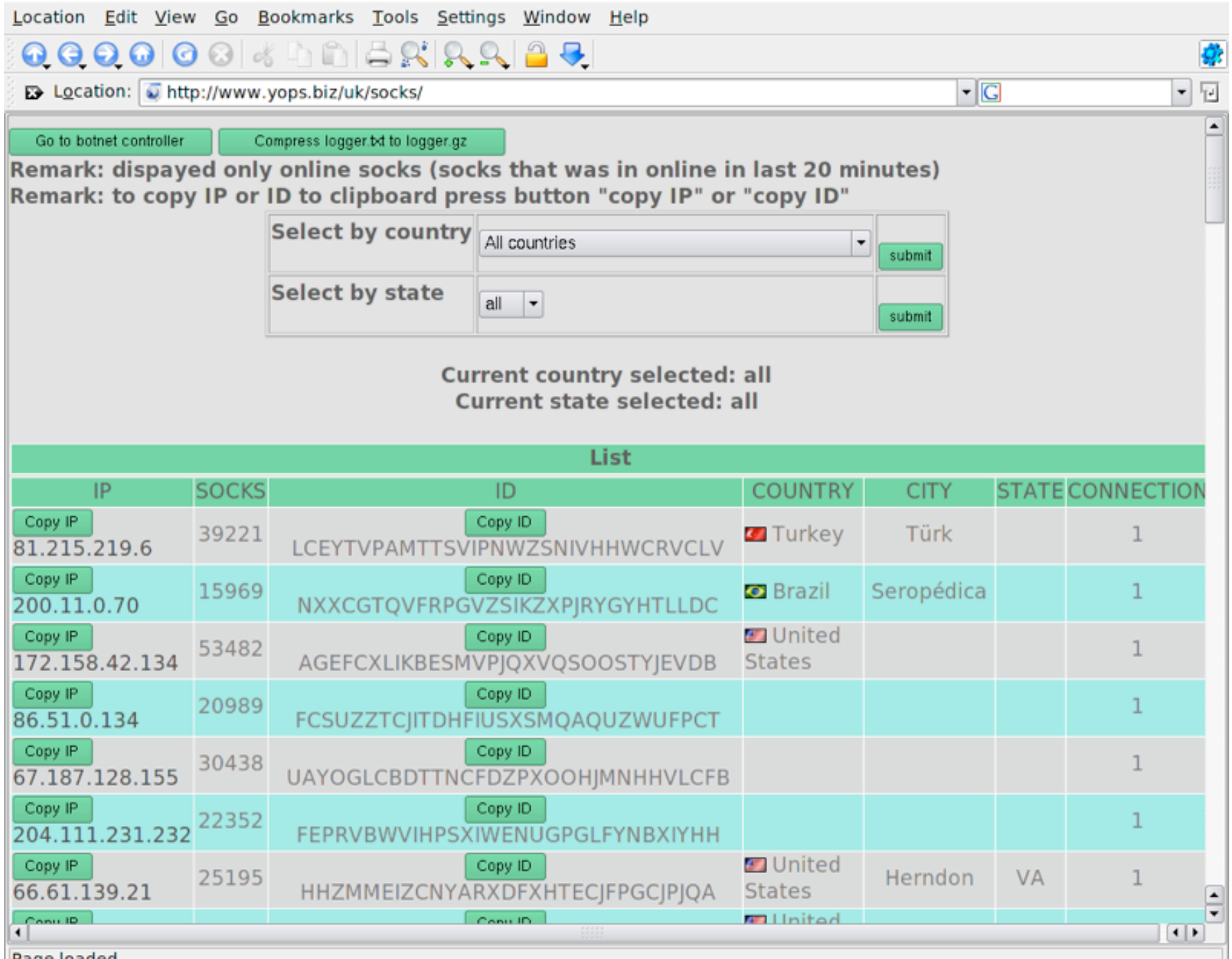
# Visualizing Event Data

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

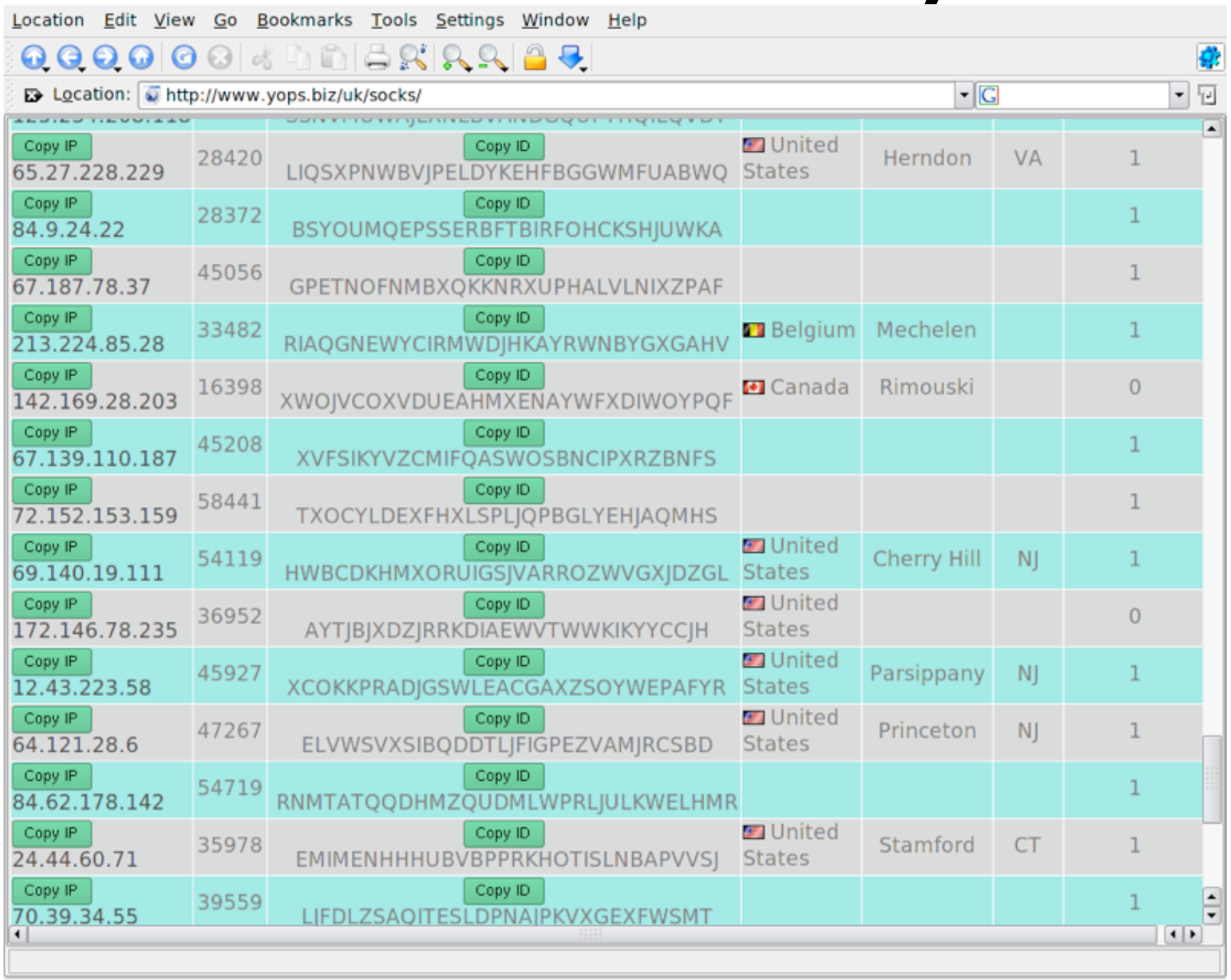
# Annotomy

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

# Controller View

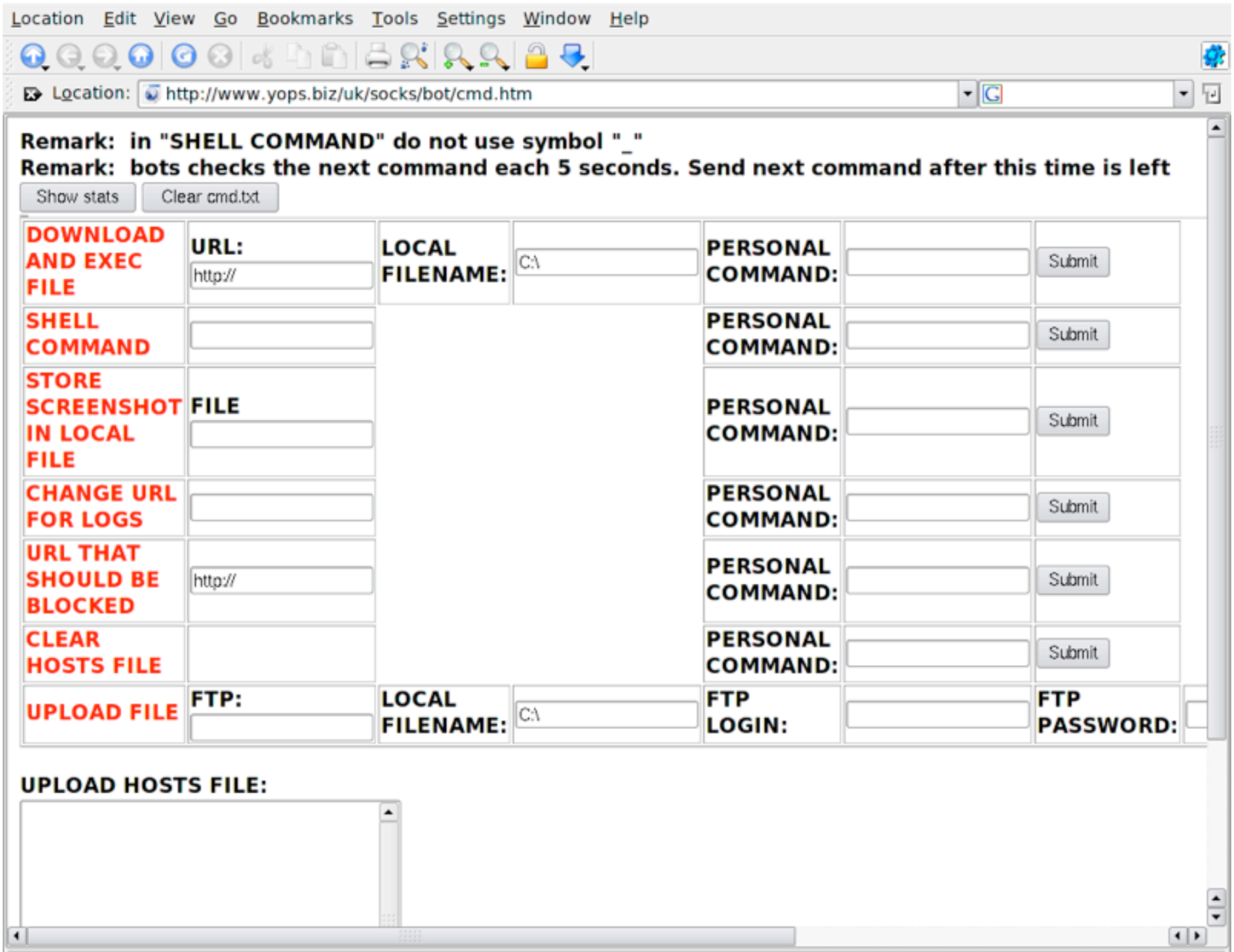


# SOCKS Proxy




| | | | | | | |
|---|---|---|---|---|---|---|
| Copy IP 65.27.228.229 | 28420 | Copy ID LIQSXPNWBVJPELDYKEHFBGGWMFUABWQ | United States | Herndon | VA | 1 |
| Copy IP 84.9.24.22 | 28372 | Copy ID BSYOUMQEPSSERBFTBIRFOHCKSHJUWKA | | | | 1 |
| Copy IP 67.187.78.37 | 45056 | Copy ID GPETNOFNMBXQKKNRXUPHALVLNIXZPAF | | | | 1 |
| Copy IP 213.224.85.28 | 33482 | Copy ID RIAQGNEWYCIRMWDJHKAYRWNBYGXGAHV | Belgium | Mechelen | | 1 |
| Copy IP 142.169.28.203 | 16398 | Copy ID XWOJVCOXVDUEAHMXENAYWFXDIWOYPQF | Canada | Rimouski | | 0 |
| Copy IP 67.139.110.187 | 45208 | Copy ID XVFSIKYVZCMIFQASWOSBNCIPXRZBNFS | | | | 1 |
| Copy IP 72.152.153.159 | 58441 | Copy ID TXOCYLDEXFHXLSPLJQPBGLYEHJAQMHS | | | | 1 |
| Copy IP 69.140.19.111 | 54119 | Copy ID HWBCDKHMXORUIGSJVARROZWVGXJDZGL | United States | Cherry Hill | NJ | 1 |
| Copy IP 172.146.78.235 | 36952 | Copy ID AYTJBJXDZJRRKDIAEWVTWWKIKYYCCJH | United States | | | 0 |
| Copy IP 12.43.223.58 | 45927 | Copy ID XCOKKPRADJGSWLEACGAXZSOYWEPAFYR | United States | Parsippany | NJ | 1 |
| Copy IP 64.121.28.6 | 47267 | Copy ID ELVWSVXSIBQDDTLJFIGPEZVAMJRCSBD | United States | Princeton | NJ | 1 |
| Copy IP 84.62.178.142 | 54719 | Copy ID RNMTATQQDHMZQUDMLWPRLJULKWELHMR | | | | 1 |
| Copy IP 24.44.60.71 | 35978 | Copy ID EMIMENHHHUBVBPPRKHOTISLNBAPVVSJ | United States | Stamford | CT | 1 |
| Copy IP 70.39.34.55 | 39559 | Copy ID LIFDLZSAQITESLDPNAIPKVXGEXFWSMT | | | | 1 |

# Other Capabilities



# 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 wellsfargo verison t-moble 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

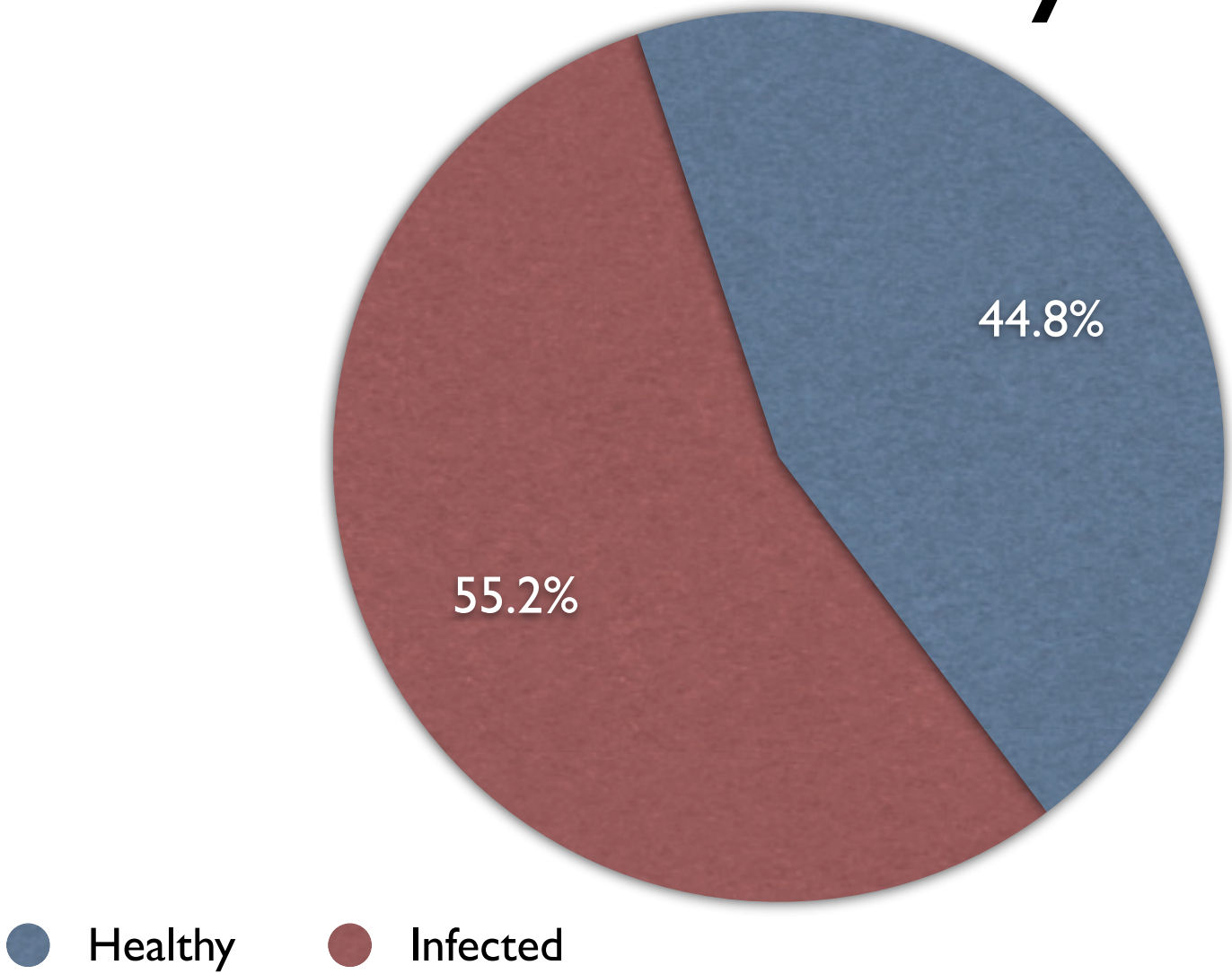
# What is it worth?

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

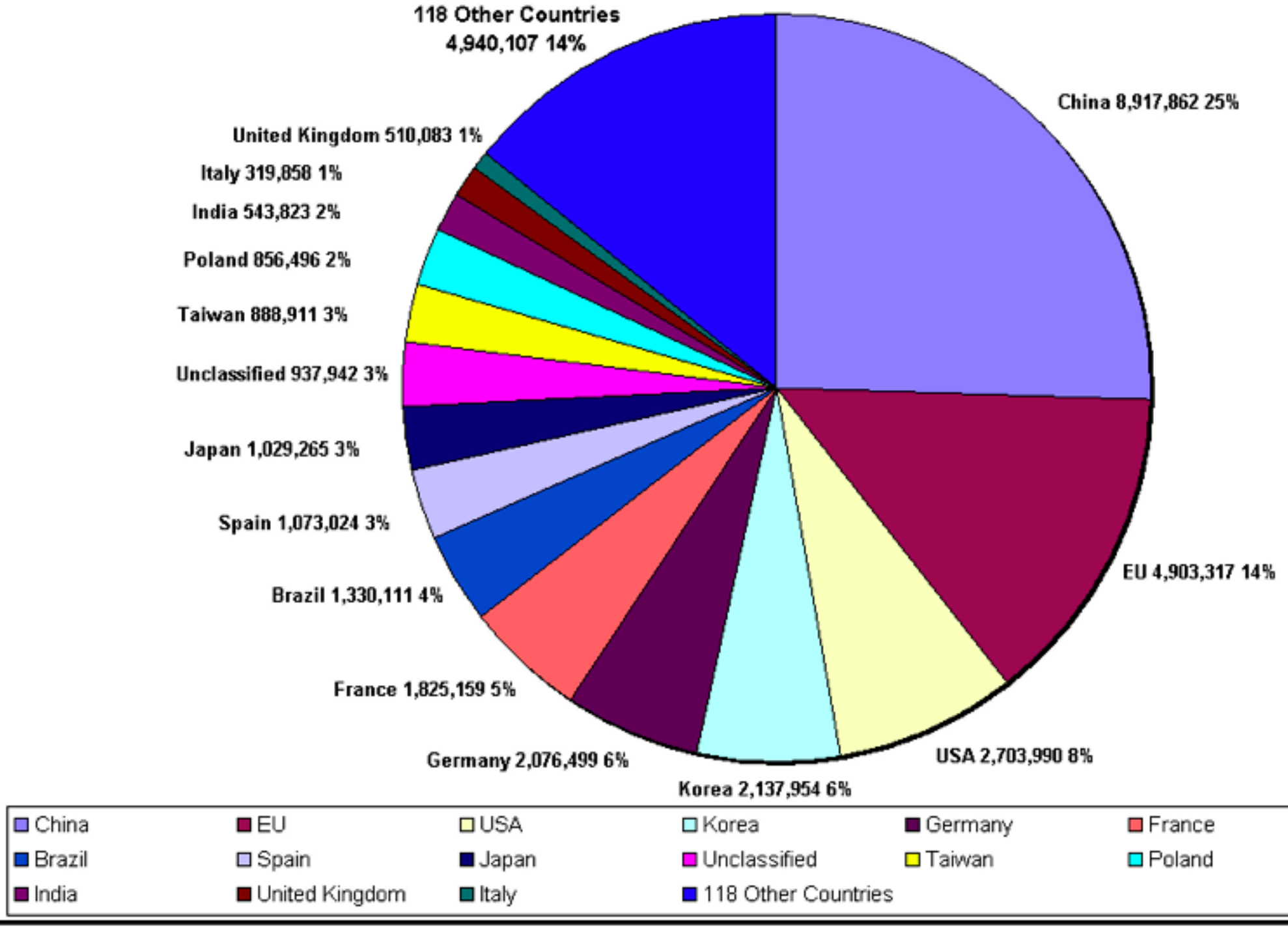
# Trends and Statistics

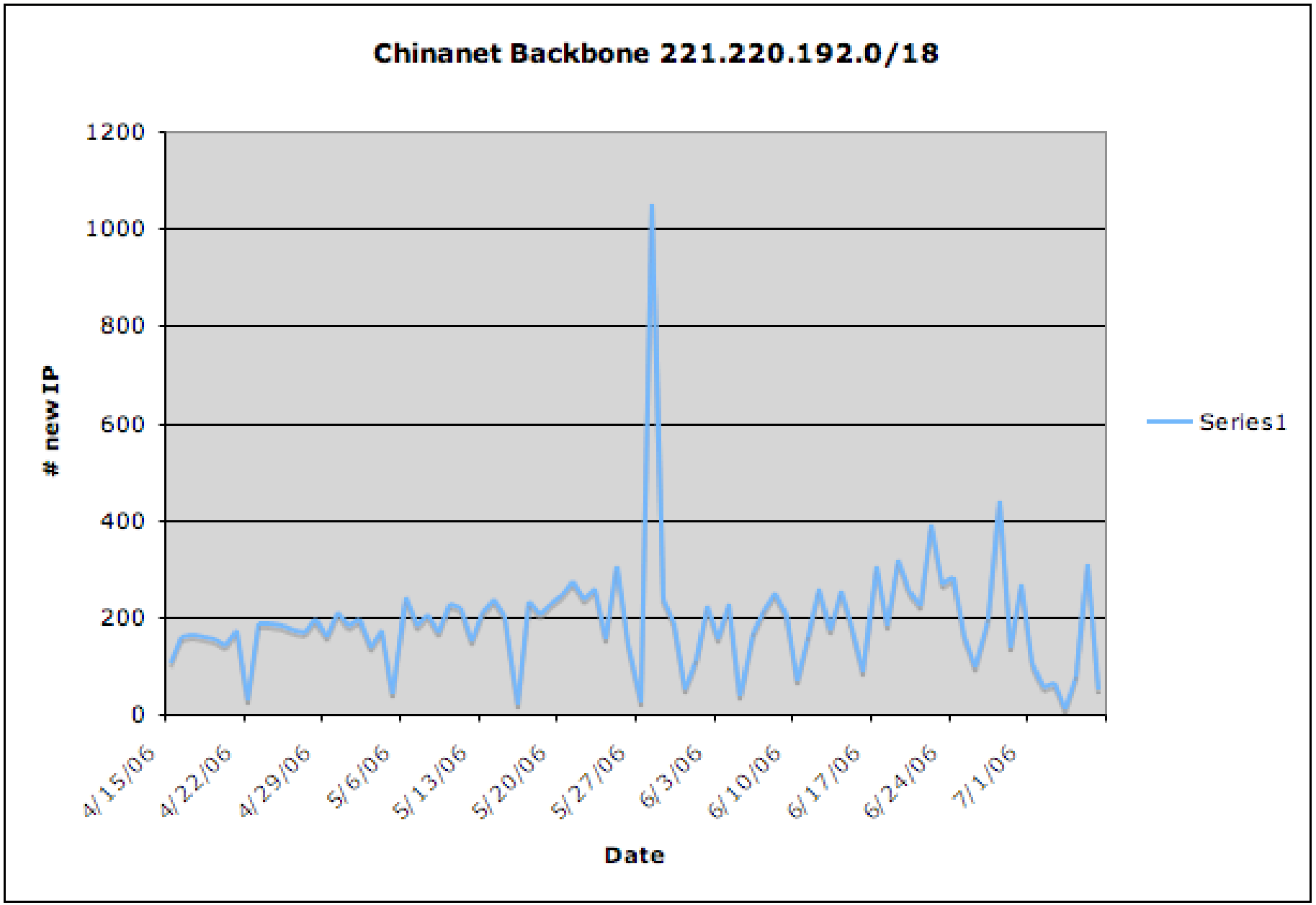
- Reviewed 101 Million events over 6 months
- 48M unique ipv4 address
- Spans 12,452 of 19,000 ASN
- Average rate of 267,489 new infections per day.

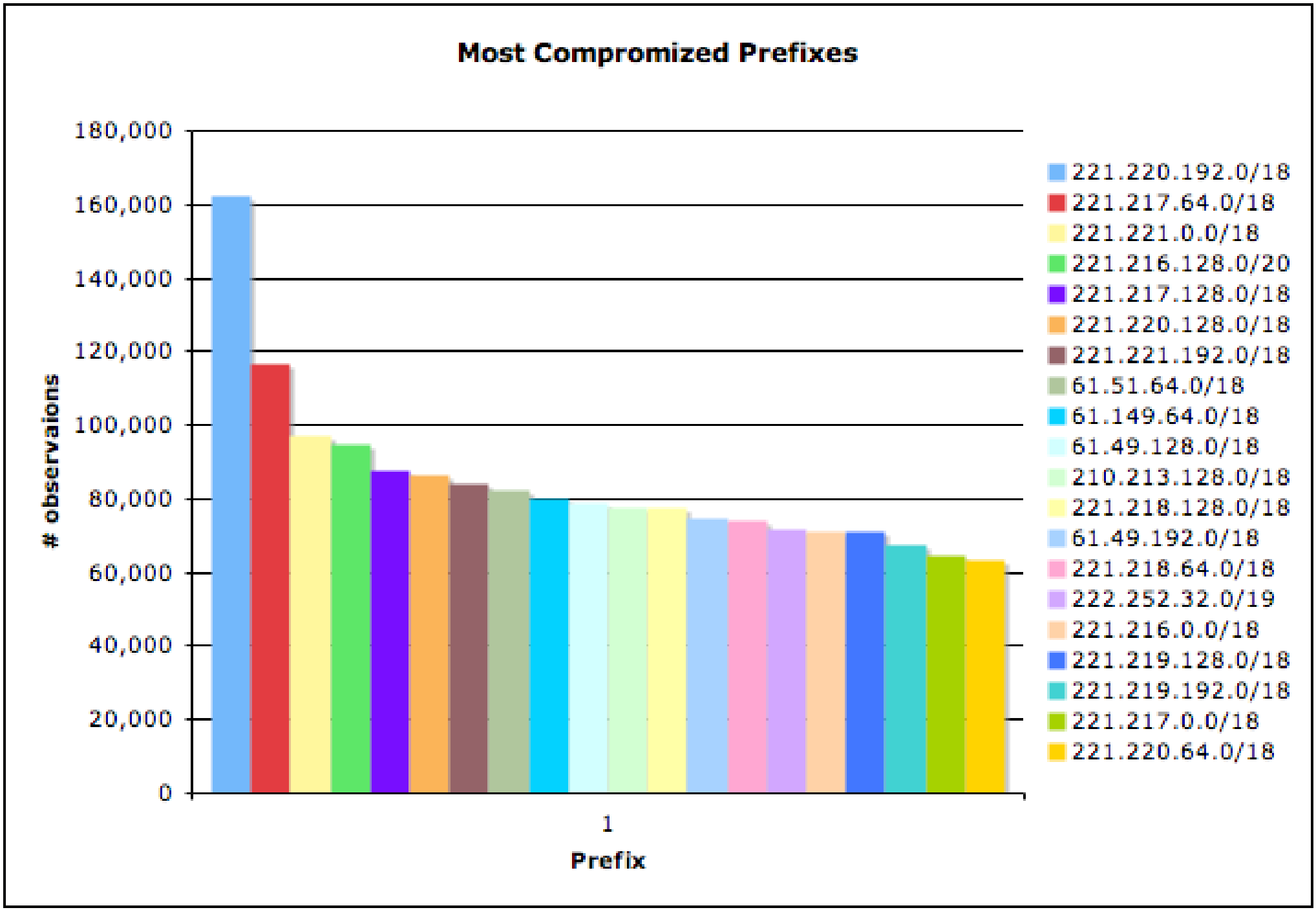
# Routed Autonomous Systems



# Top 15 Countries with the Most Compromised Systems (1st Half 2006)




Chinanet Backbone 221.220.192.0/18
1200
1000
800
600
400
200
0
# new IP
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
Date
Series1


Most Compromized Prefixes
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
# observaions
1
Prefix
221.220.192.0/18
221.217.64.0/18
221.221.0.0/18
221.216.128.0/20
221.217.128.0/18
221.220.128.0/18
221.221.192.0/18
61.51.64.0/18
61.149.64.0/18
61.49.128.0/18
210.213.128.0/18
221.218.128.0/18
61.49.192.0/18
221.218.64.0/18
222.252.32.0/19
221.216.0.0/18
221.219.128.0/18
221.219.192.0/18
221.217.0.0/18
221.220.64.0/18

# Tools

- REACTb 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)