

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

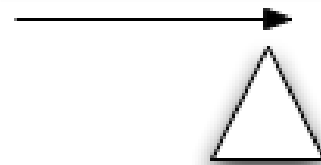
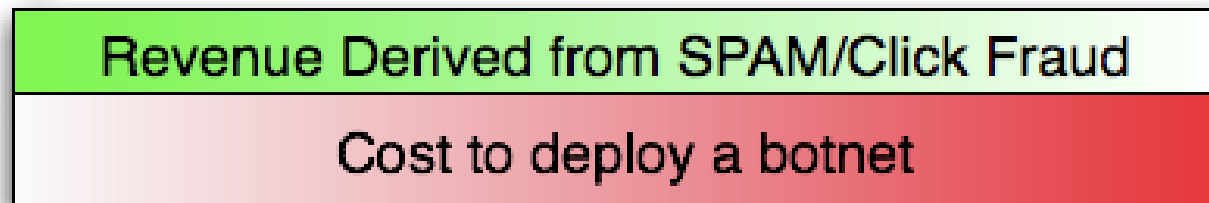
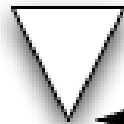
woody-maclen

economic theory of abuse

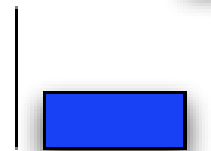
Overlap



Revenue '06



Costs '06

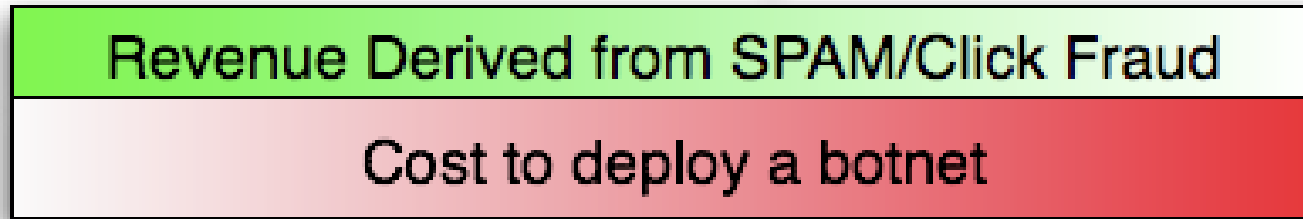
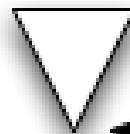


Incentive

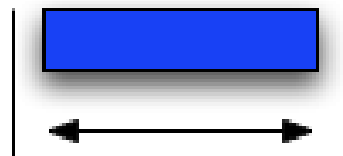
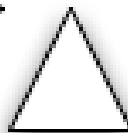
Gap



Revenue '09



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

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://www.yops.biz/uk/socks/

[Go to botnet controller](#) [Compress logger.txt to logger.gz](#)

Remark: displayed only online socks (socks that was 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

List						
IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION
<input type="button" value="Copy IP"/> 81.215.219.6	39221	<input type="button" value="Copy ID"/> LCEYTVPAMTTSVIPNWZSNIVHHWCRVCLV	Turkey	Türk		1
<input type="button" value="Copy IP"/> 200.11.0.70	15969	<input type="button" value="Copy ID"/> NXXCGTQVFRPGVZSIKZXPJRYGYHTLLDC	Brazil	Seropédica		1
<input type="button" value="Copy IP"/> 172.158.42.134	53482	<input type="button" value="Copy ID"/> AGEFCXLIKESMVPJQXVQSOOSTYJEVDB	United States			1
<input type="button" value="Copy IP"/> 86.51.0.134	20989	<input type="button" value="Copy ID"/> FCSUZZTCJITDHFUSXSMQAQUZWUFPCT				1
<input type="button" value="Copy IP"/> 67.187.128.155	30438	<input type="button" value="Copy ID"/> UAYOGLCBDTTNCDFZPXOOHJMNHHVLCFB				1
<input type="button" value="Copy IP"/> 204.111.231.232	22352	<input type="button" value="Copy ID"/> FEPRVBWVIHPSXIWENUGPGLFYNBXIYHH				1
<input type="button" value="Copy IP"/> 66.61.139.21	25195	<input type="button" value="Copy ID"/> HHZMMEIZCNYARXDFXHTECFJPGCJPJQA	United States	Herndon	VA	1
<input type="button" value="Copy IP"/>		<input type="button" value="Copy ID"/>	United States			

Page loaded

SOCKS Proxy

Copy IP	Copy ID	Country	Location	Value
65.27.228.229	28420	United States	Herndon VA	1
84.9.24.22	28372			1
67.187.78.37	45056			1
213.224.85.28	33482	Belgium	Mechelen	1
142.169.28.203	16398	Canada	Rimouski	0
67.139.110.187	45208			1
72.152.153.159	58441			1
69.140.19.111	54119	United States	Cherry Hill NJ	1
172.146.78.235	36952	United States		0
12.43.223.58	45927	United States	Parsippany NJ	1
64.121.28.6	47267	United States	Princeton NJ	1
84.62.178.142	54719			1
24.44.60.71	35978	United States	Stamford CT	1
70.39.34.55	39559			1

Other Capabilities

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <http://www.yops.biz/uk/socks/bot/cmd.htm>

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

Show stats Clear cmd.txt

DOWNLOAD AND EXEC FILE	URL: <input type="text" value="http://"/>	LOCAL FILENAME: <input type="text" value="CA"/>	PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
SHELL COMMAND	<input type="text"/>		PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
STORE SCREENSHOT IN LOCAL FILE	FILE <input type="text"/>		PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
CHANGE URL FOR LOGS	<input type="text"/>		PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
URL THAT SHOULD BE BLOCKED	<input type="text" value="http://"/>		PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
CLEAR HOSTS FILE			PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
UPLOAD FILE	FTP: <input type="text"/>	LOCAL FILENAME: <input type="text" value="CA"/>	FTP LOGIN: <input type="text"/>	FTP PASSWORD: <input type="text"/>

UPLOAD HOSTS FILE:

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)

Effectuated 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 walmart
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

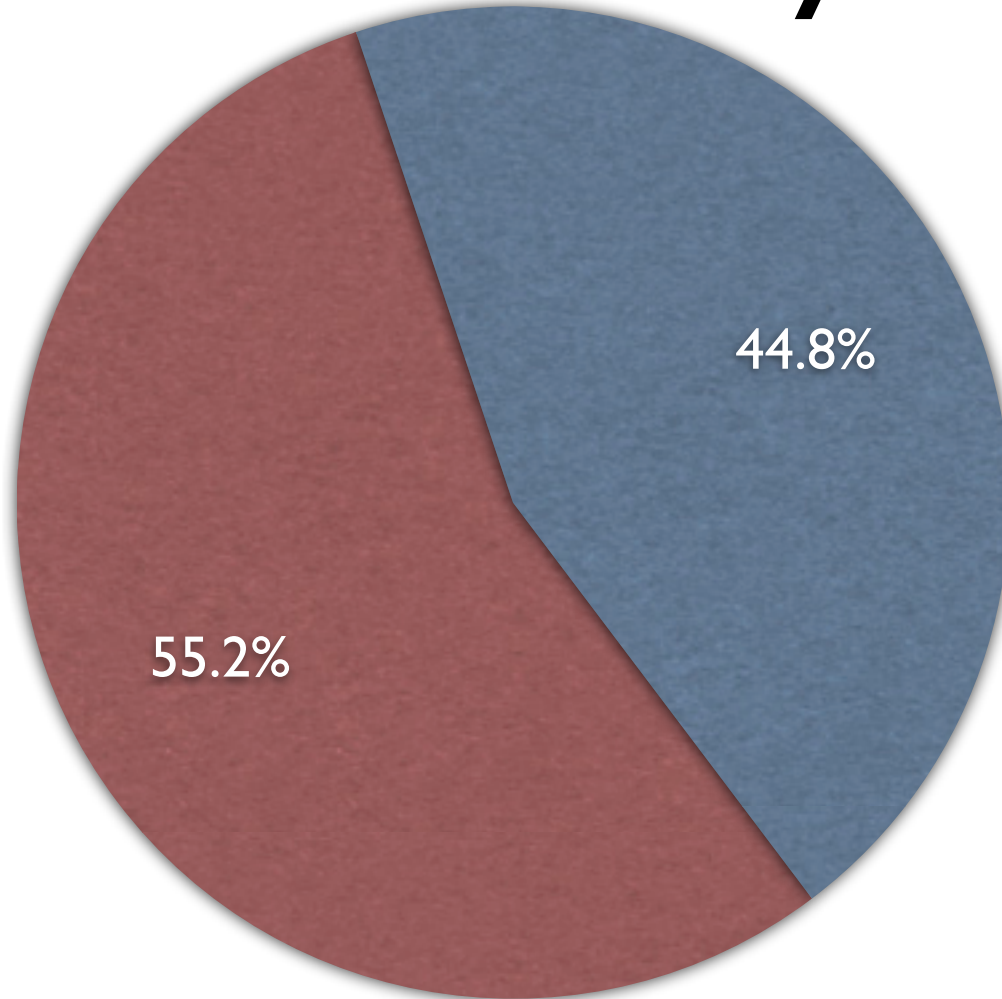
What is it worth?

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

Trends and Statistics

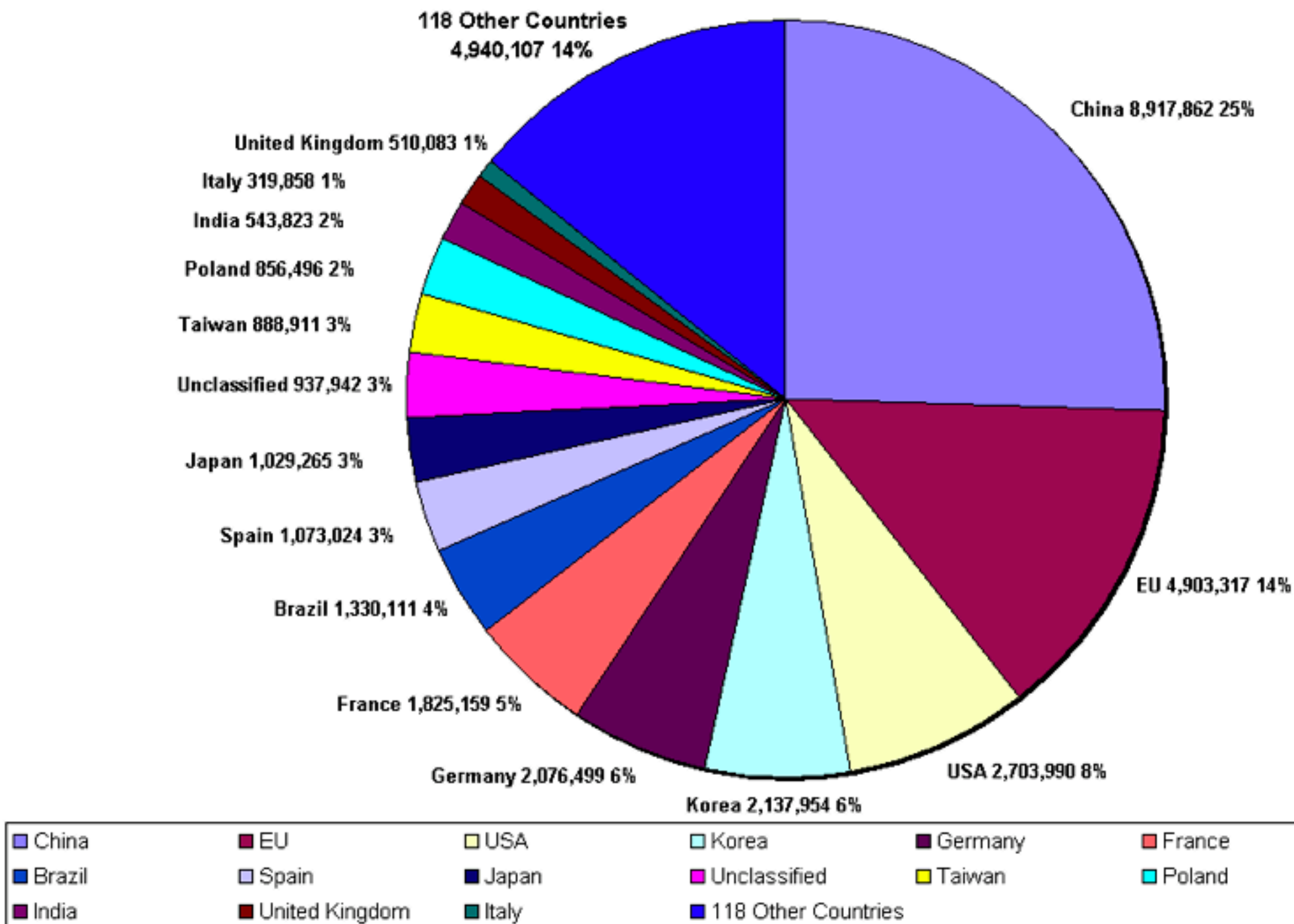
- Reviewed 101 Million events over 6 months
- 48M unique ipv4 address
- Spans 12,452 of 19,000 ASN
- Average rate of 267,489 new infections per day.

Routed Autonomous Systems

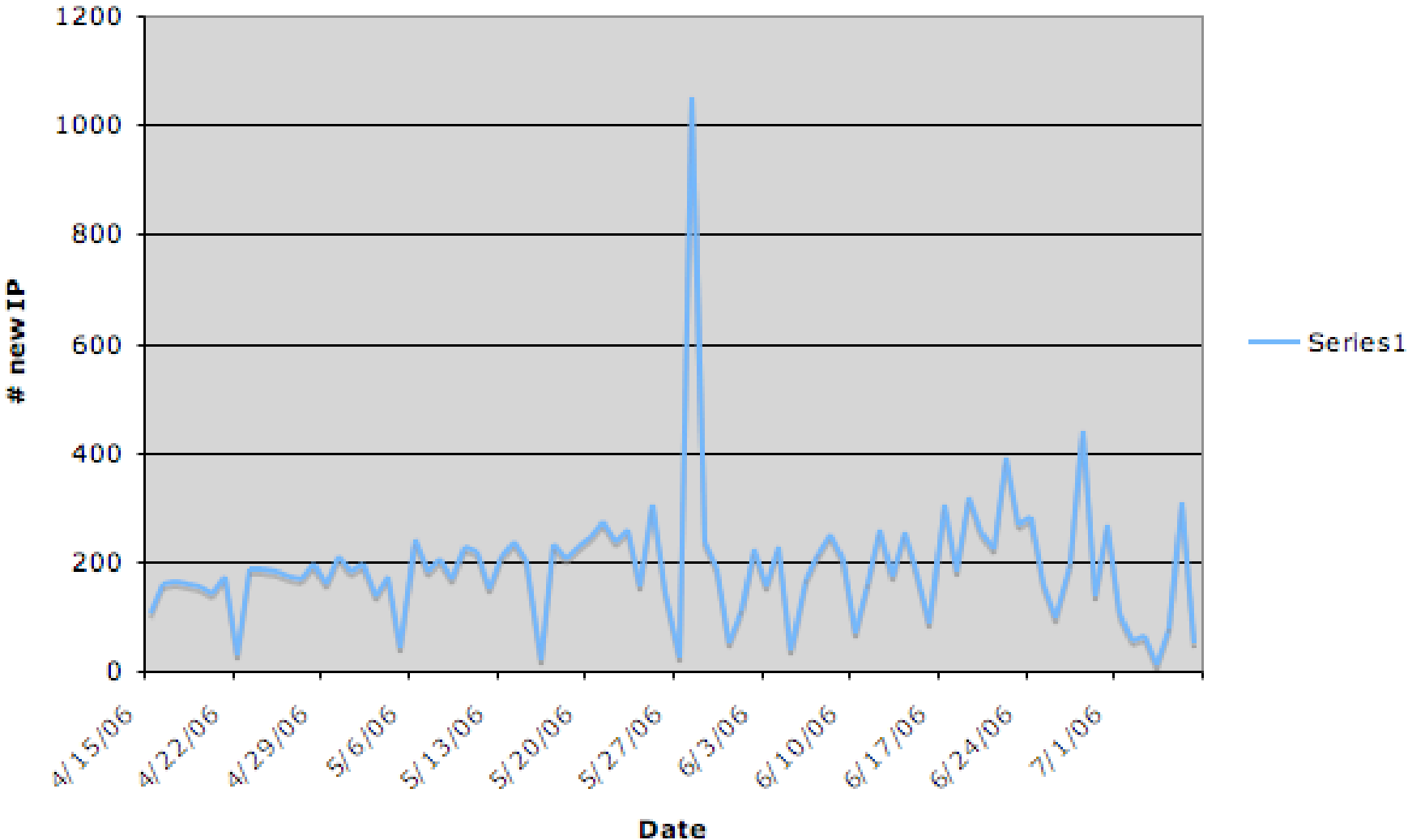


● Healthy ● Infected

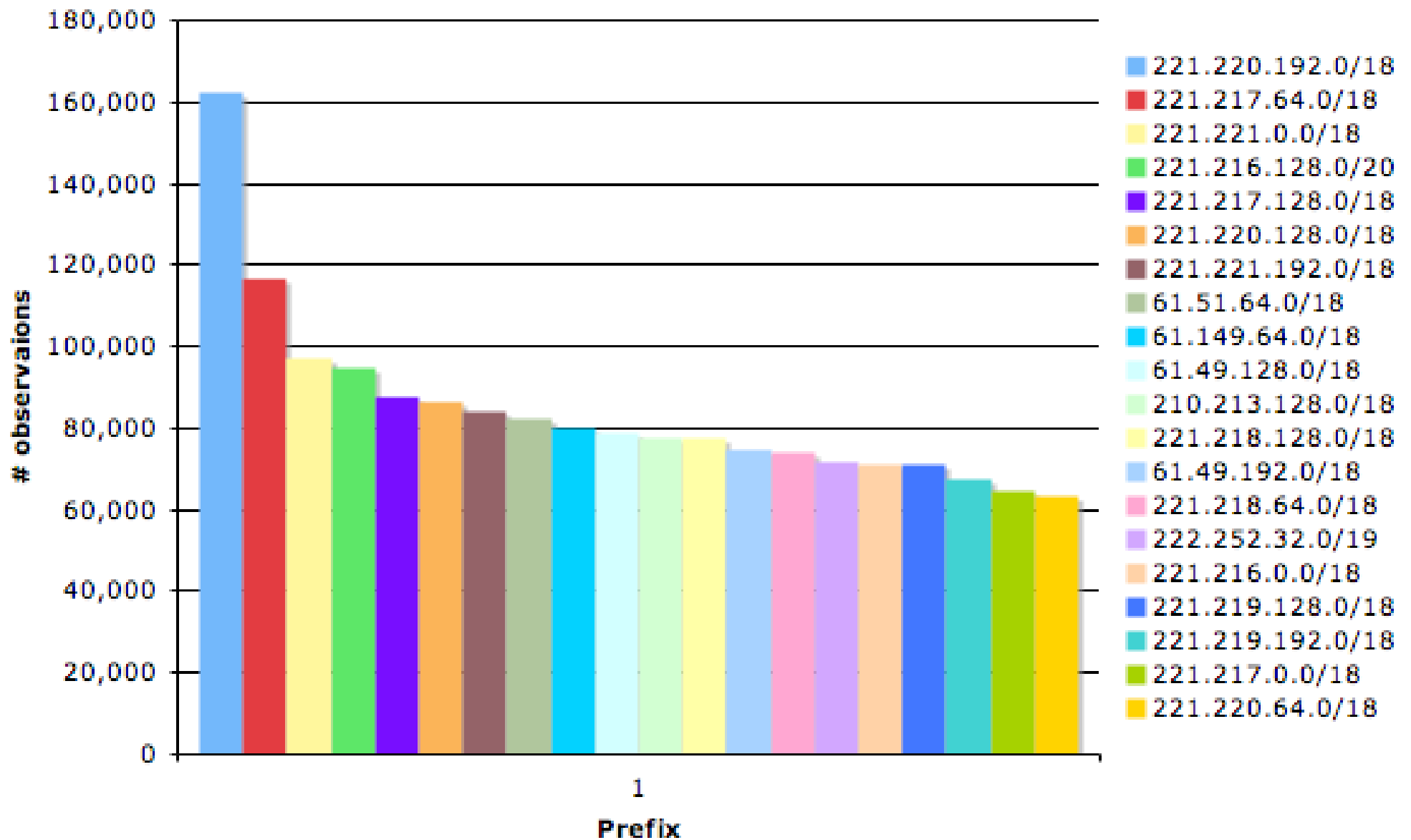
Top 15 Countries with the Most Compromised Systems (1st Half 2006)



Chinanet Backbone 221.220.192.0/18



Most Compromized Prefixes



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)