

Botnets and the Global Infection Rate

Anticipating Security Failures

June 6, 2007

Stanford University

EE Dep Computer Systems Colloquium

Palo Alto, CA

Rick Wesson

CEO, Support Intelligence, LLC

Overview

- Problem Statement and Definitions
- Global Network Analysis
- Anatomy of a Bot Network
- Command and Control
- Victims and Villains
- Anticipating Security Failures

Problem Statement

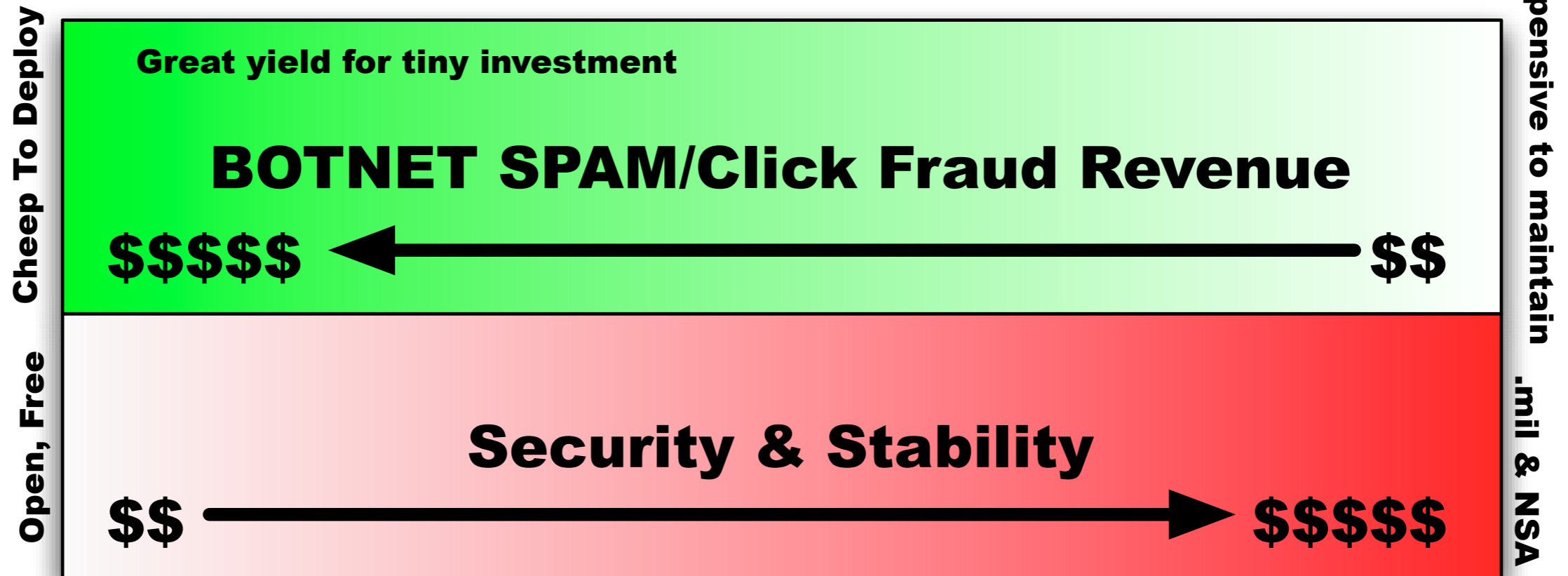
- It is often hard to understand when a device on your network has been owned until it has acted out.
- the number of newly infected systems is growing faster than any organically based infectious disease ever documented.
- 4.3M new human AIDS cases in 2006

Definitions

- Abuse or Malicious Behavior is
 - DDoS
 - Click-Fraud, Auction Fraud
 - Hosting Open {proxies, relays}
 - Splogs, Flogs, Phish, Identity Theft
 - BGP Route Hijacking {bogons}
 - SPAM/UCE via Botnets, C&C

Economics of abuse

Cost to deploy a botnet



Cost to secure a network

Infection Vectors

- Email Attachments
- Instant Messages
- Web Pages
- P2P File sharing networks
- Network

Global Identifiers

- 8.1M routed /24 blocks
- 140M Domains
- 22K ASN
- 200K Routes
- 2.2M Events/day

Automated Forensics

- HoneyPots, Darknets, Massive SpamTrap
- Partners { cisco, ironPort, postini }
- Community Partners: Spamcop, SpamHaus, other DNSRBLs
- ISPs, Universities, Security Researchers
- 135 data sources
- BGP, RIRs, Registrars, Registries(cnobiu)
- Mine DNS, 78M Domains

Anatomy of an insider threat

- Controller Capabilities
 - Socks Proxy
 - Web Front-end
 - Commands and Management
- Data Ex-filtration
 - 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: [submit](#)

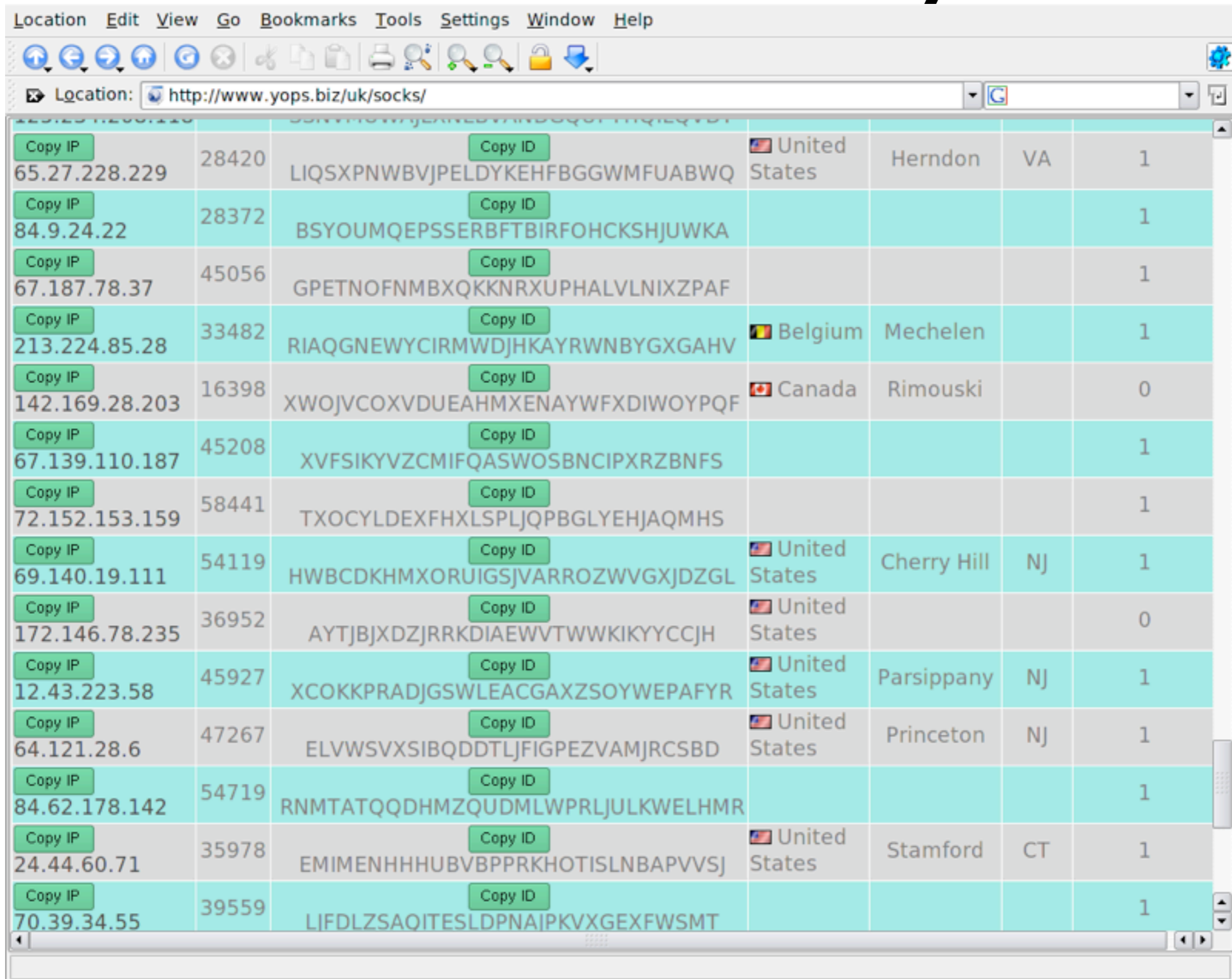
Select by state: [submit](#)

Current country selected: all
Current state selected: all

List						
IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION
Copy IP 81.215.219.6	39221	Copy ID LCEYTVPAMTTVIPNWZSNIVHHWCRVCLV	Turkey	Türk		1
Copy IP 200.11.0.70	15969	Copy ID NXXCGTQVFRPGVZSIKZXPJRYGYHTLLDC	Brazil	Seropédica		1
Copy IP 172.158.42.134	53482	Copy ID AGEFCXLIKESMVPJQXVQSOOSTYJEVDB	United States			1
Copy IP 86.51.0.134	20989	Copy ID FCSUZZTCJITDHFIOUSXSMQAQUZWUFPC				1
Copy IP 67.187.128.155	30438	Copy ID UAYOGLCBDTTNCFDZPXOOHJMNHHVLCFB				1
Copy IP 204.111.231.232	22352	Copy ID FEPRVBWVIHPSXIWENUGPGLFYNBXIYHH				1
Copy IP 66.61.139.21	25195	Copy ID HHZMMEIZCNYARXDFXHTECFPGCJPJQA	United States	Herndon	VA	1
Copy IP		Copy ID	United States			

Page loaded

SOCKS Proxy



The screenshot shows a web browser window with the address bar containing <http://www.yops.biz/uk/socks/>. The browser interface includes a menu bar (Location, Edit, View, Go, Bookmarks, Tools, Settings, Window, Help) and a toolbar with navigation and utility icons. The main content area displays a table of socks proxy servers.

Copy IP	Copy ID	Copy ID	Country	City	State	Count
65.27.228.229	28420	LIQSPNWBVJPELDYKEHFBGGWMFUABWQ	United States	Herndon	VA	1
84.9.24.22	28372	BSYOUMQEPSSERBFTBIRFOHCKSHJUWKA				1
67.187.78.37	45056	GPETNOFNMBXQKKNRXUPHALVLNIXZPAF				1
213.224.85.28	33482	RIAQGNEWYCIRMWDJHKAYRWNBYGXGAHV	Belgium	Mechelen		1
142.169.28.203	16398	XWOJVCOXVDUEAHMXENAYWFXDIWOYPQF	Canada	Rimouski		0
67.139.110.187	45208	XVFSIKYVZCMIFQASWOSBNCIPXRZBNFS				1
72.152.153.159	58441	TXOCYLDEXFHXLSPJQPBGLEYHJMQMHS				1
69.140.19.111	54119	HWBCDKHMXORUIGSJARROZWVGXJDZGL	United States	Cherry Hill	NJ	1
172.146.78.235	36952	AYTJBXJXDZJRRKDIAEWVTWWKIKYYCCJH	United States			0
12.43.223.58	45927	XCOKKPRADJGSWLEACGAXZSOYWEPAYR	United States	Parsippany	NJ	1
64.121.28.6	47267	ELVWSVXSIBQDDTLJFIGPEZVAMJRCSBD	United States	Princeton	NJ	1
84.62.178.142	54719	RNMTATQQDHMZQUDMLWPRLJULKWELHMR				1
24.44.60.71	35978	EMIMENHHUBVBPPRKHOTISLNBAPVVSJ	United States	Stamford	CT	1
70.39.34.55	39559	LIFDLZSAOITESLDPNAIPKVXGEXFWSMT				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="C:\"/>	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	<input type="text"/>		PERSONAL COMMAND: <input type="text"/>	<input type="button" value="Submit"/>
UPLOAD FILE	FTP: <input type="text"/>	LOCAL FILENAME: <input type="text" value="C:\"/>	FTP LOGIN: <input type="text"/>	FTP PASSWORD: <input type="text"/>

UPLOAD HOSTS FILE:

do Bots send SPAM?

SPAMBOT CONTROL PANEL

SENDER NAME	<input type="text"/>
SUBJECT	<input type="text"/>
MAIL FROM	<input type="text"/>
URL FOR MESSAGE BODY	<input type="text"/>
URL FOR SPAMLIST	<input type="text"/>
MACHINE ID	<input type="text"/>

SUBMIT

Data Ex-filtration

REMOTE ADDRESS: 172.189.109.174

ID: BPAQZLZBBLUWRYGVSXOTJHALUVNRBXS

TIMESTAMP: 25\5 14:0:51

Copyright By Smash and SARS

From: MATTHEW

IP address: 10.0.0. [System information]

Windows XP Internet Explorer 6.0.2900.21

MAIL: POP383EE26C0

Chal89/PAUL

10.0.0.4 <http://petiteteeniemia.join4free.com/>

_B64S_bm9kZWQvNjYvbW92aWVsYW5kL0FBQS9odHRwJTnBJTJGJTJGd3d3LnNl
eGJyb2FkY2FzdGVyLmNvbSUyRi8xMTMxNDk3OTQ2L2ZBdi5UZGY5SEJscUU=_E/

Login: chal89@aol.com Pass: chal89

10.0.0.4 <http://sib1.od2.com/common/Framework.aspx> Login: chal89 Pass: mat123

10.0.0.4 <http://uk.mcafee.com/root/login.asp>

*** Protected Storage Data ends ***

Analysis of Data Ex-Filtrated (30 days)

- 793 uniquely infected systems
- 17,195 data captures
- 35,867 form logs (multiple per data capture)
- 100% MS Windows XP IE 6.0.2XX
- 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)

Ex-filtration File Contents

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

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

Sample of Affected Companies

- 1,239 companies/domains
- 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
citibank americanexpress sprintpcs usbank
esurance wal-mart ticketweb us.army.mil

How botnets affect corporations

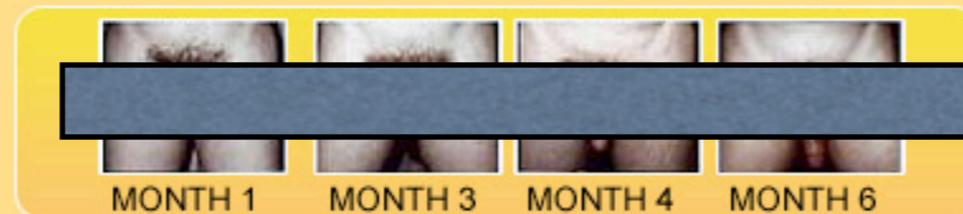
HP DHL Airtouch Cellular Agilent, CNet
Lawrence Berkeley Labs AutoDesk,
WellsFargo, Charles Schwab Intuit Mercury
Interactive The Gap Bank of America Veritas
Sprint SLAC Nokia E-Trade, Epinions
Friendster Chevron-Texaco

see <http://blog.support-intelligence.com/>

**How would you like a
MUCH BIGGER PENIS?
Gain upto 2-3 inches!!***

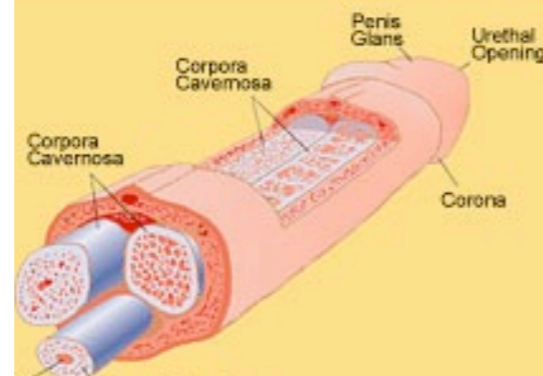
**NATURAL
AND SAFE**

**ADD 3 INCHES IN LENGTH!
GAIN AN EXTRA 20% IN THICKNESS!
PRODUCE STRONGER ERECTIONS!
HAVE MORE INTENSE ORGASMS!
HAVE A STRONGER SEXUAL DESIRE!
INCREASED SEXUAL STAMINA!**



Thanks to Prasad for sending in these pics of his results!

**MORE-SIZE HAS HELPED OVER
1,000,000
MEN AROUND THE WORLD,
GAIN INCHES...**



HOW DOES IT WORK?

The penis is made up of 3 chambers, 2 large ones on top, which is your erectile tissue (Corpora Cavemosa), and 1 smaller chamber on the bottom from which you urinate and ejaculate (Corpus Spongiosum). When you are sexually aroused, your brain releases a hormone causing blood to enter the penis and

Corporate Penis Enlargement Problem

- Botnet spam through corporate MX
- Spamvertised link that transverses 3 web servers (302 Moved Temporarily)
- Domains hosted across 3 registrars with 3 different identities and 3 distinct hosting services across USA, Germany, Russia, and China.
- Final web server hosted in China.

Corporate Espionage

- Capabilities ex-filtrate data
- Data Mining for network and hard drives
- Stealth

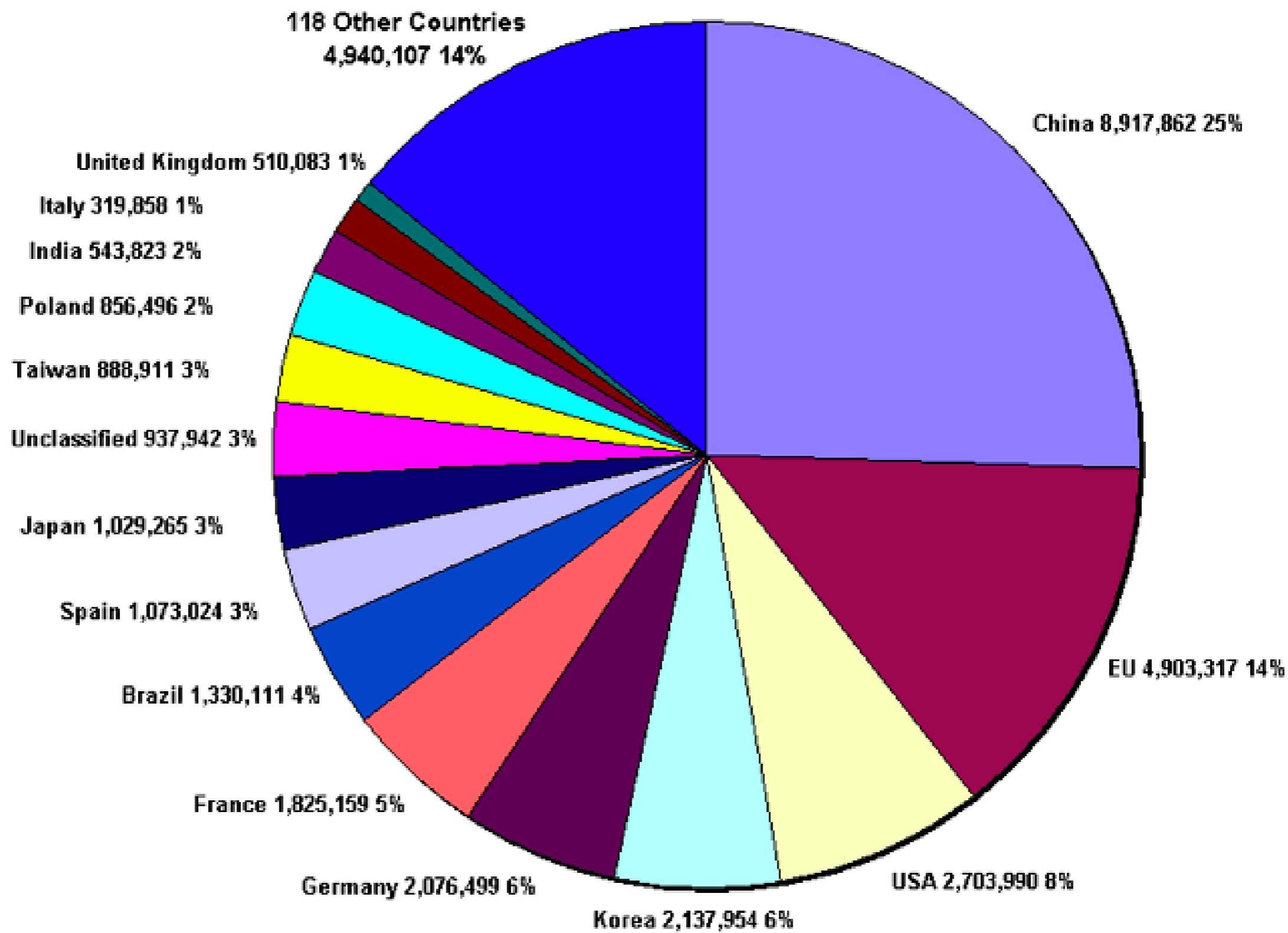
Global Scope Trends and Statistics

- Reviewed 101 Million events over 6 months
- 48M unique ipv4 address
- Spans 12,452 of 22,570 Routed ASN
- Estimated average rate of 267,489 new infections per day.
- 11,780 new AIDS infections/day

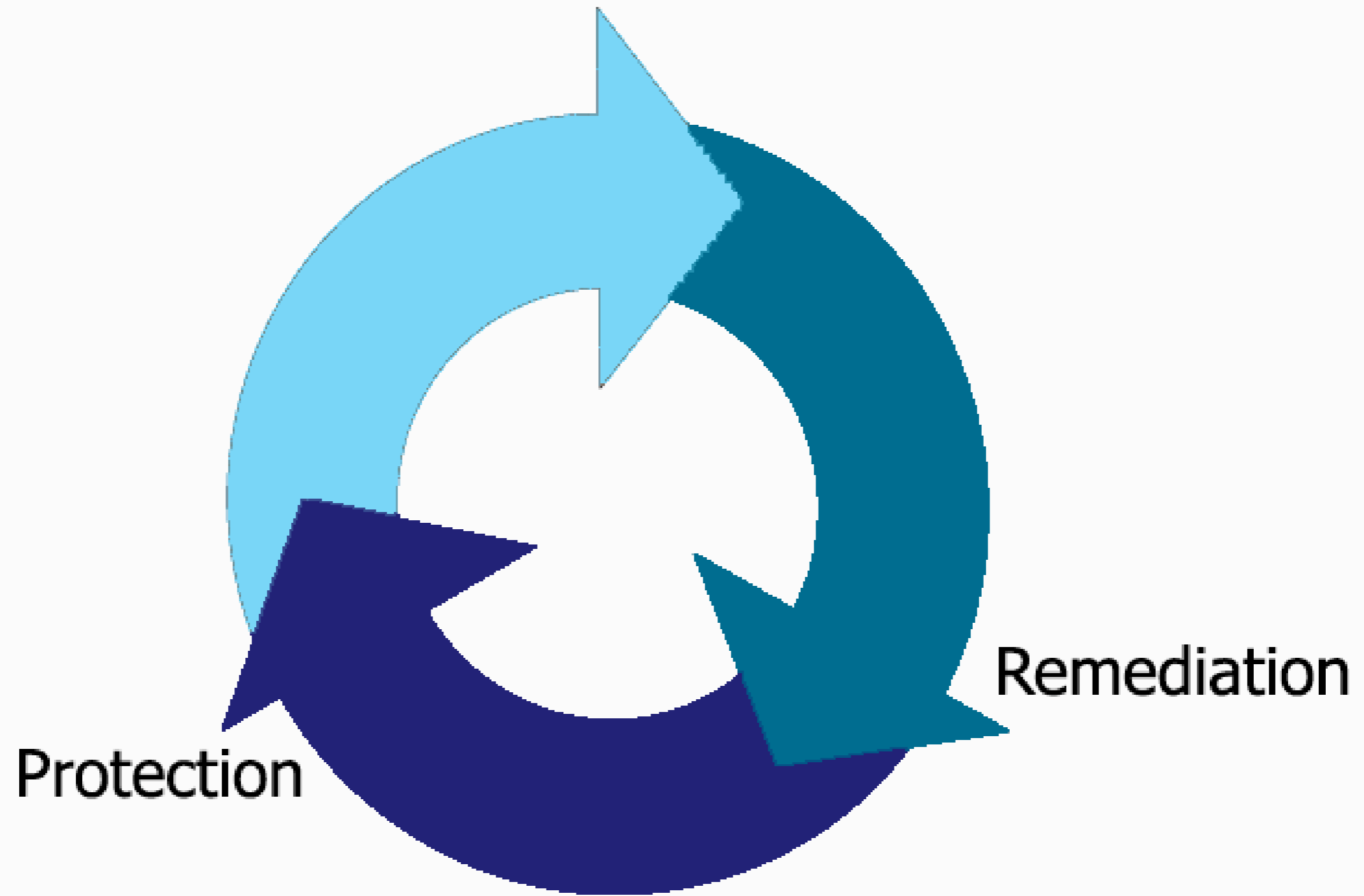
Who is Owned

- Massive infections on Broadband Networks
- Government and Educational Organizations
- Small and Mid-sized Businesses
- Russell 2000 and Fortune 500
- Everyone gets owned

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



Detection



Remediation

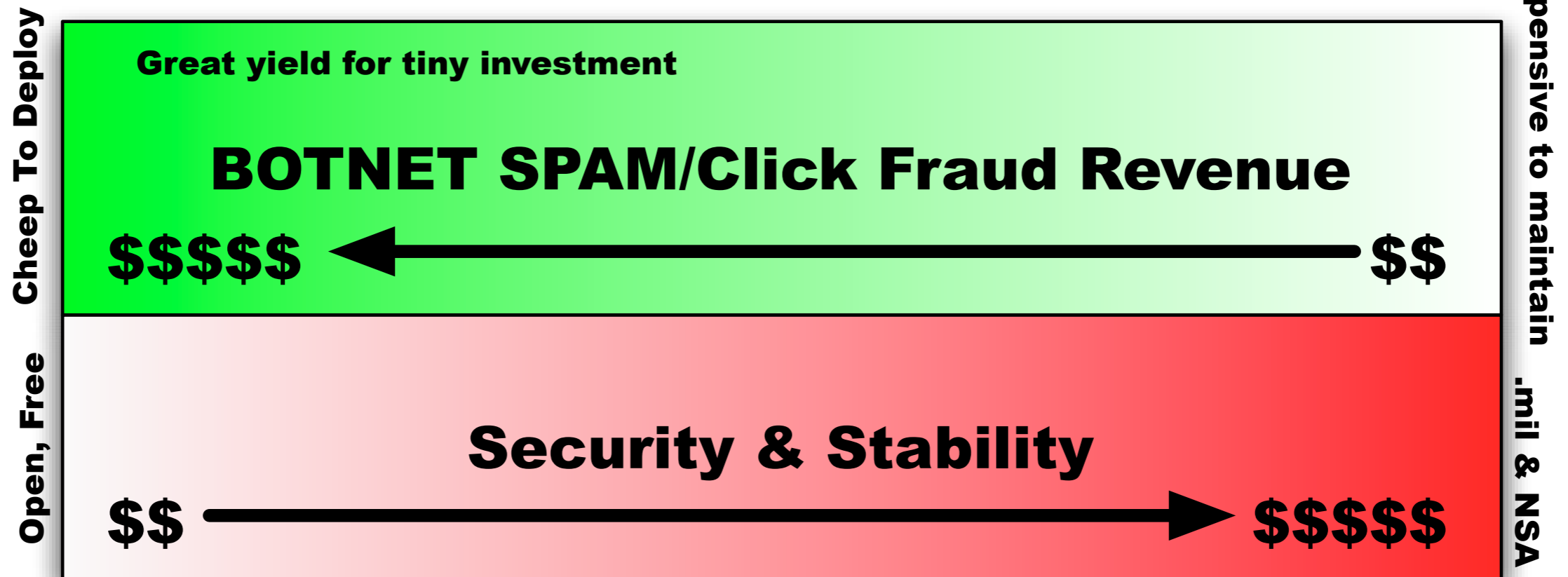
Protection

Detecting Compromised Companies

- Bank of America, Aflec, 3M
- Nationwide Insurance, Indymac Bank
- Intel, Border Group
- Clear Channel
- Toshiba, ATA Airlines
- Business Week

Economics of abuse

Cost to deploy a botnet



Cost to secure a network

Identity and Security

- Without security what is Identity?
- A good reputation is valuable, to a bot

Anticipating Failure

- Understanding security failures is much like anticipating that houses catch on fire and smoke detectors save lives.
- Security will fail, its understanding when its failed that saves your assets.

Questions

see <http://Support-Intelligence.com>

rick@Support-Intelligence.com