How The Pursuit of Truth Led Me To Selling Viagra®

Vern Paxson

International Computer Science Institute
EECS Department, University of California
Lawrence Berkeley National Laboratory
Berkeley, California USA

October 17, 2008

Outline:

- For network research, the past two decades represent a time of amazing growth and **repeated**, rapid paradigm shifts
  - Of course, you shouldn't believe this claim w/o **measurements** to back it up!

- A personal view:
  - From network measurement to detecting attacks
  - From manual attacks ⇒ worms ⇒ bots ⇒ spam
  - Why all this leads to selling Viagra

First, some acknowledgments:

- ICSI: Mark Allman, Christian Kreibich, Robin Sommer, Nicholas Weaver
- LBL: Craig Leres, Brian Tierney, Jim Rothfuss, Dwayne Ramsey, et al
- UC Berkeley: Weidong Cui (now MSR)
- UC San Diego: Stefan Savage, Geoff Voelker, Chris Kanich, Kirill Levchenko, Brandon Enright

Part I

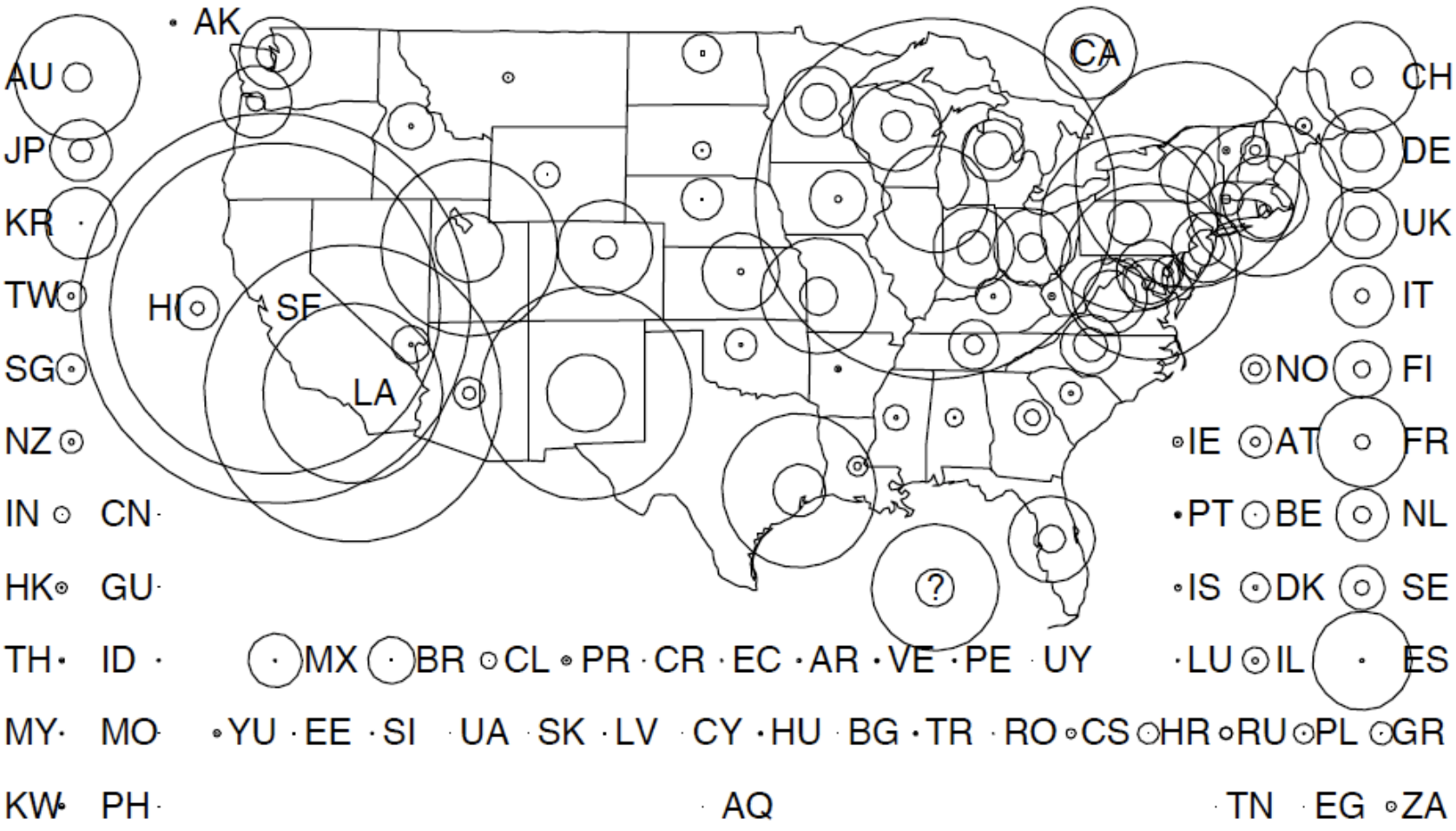
Pursuit of Truth +
Phobia of Being Fooled =
Thirst for Data

As ICSI Develops, So Does the Internet

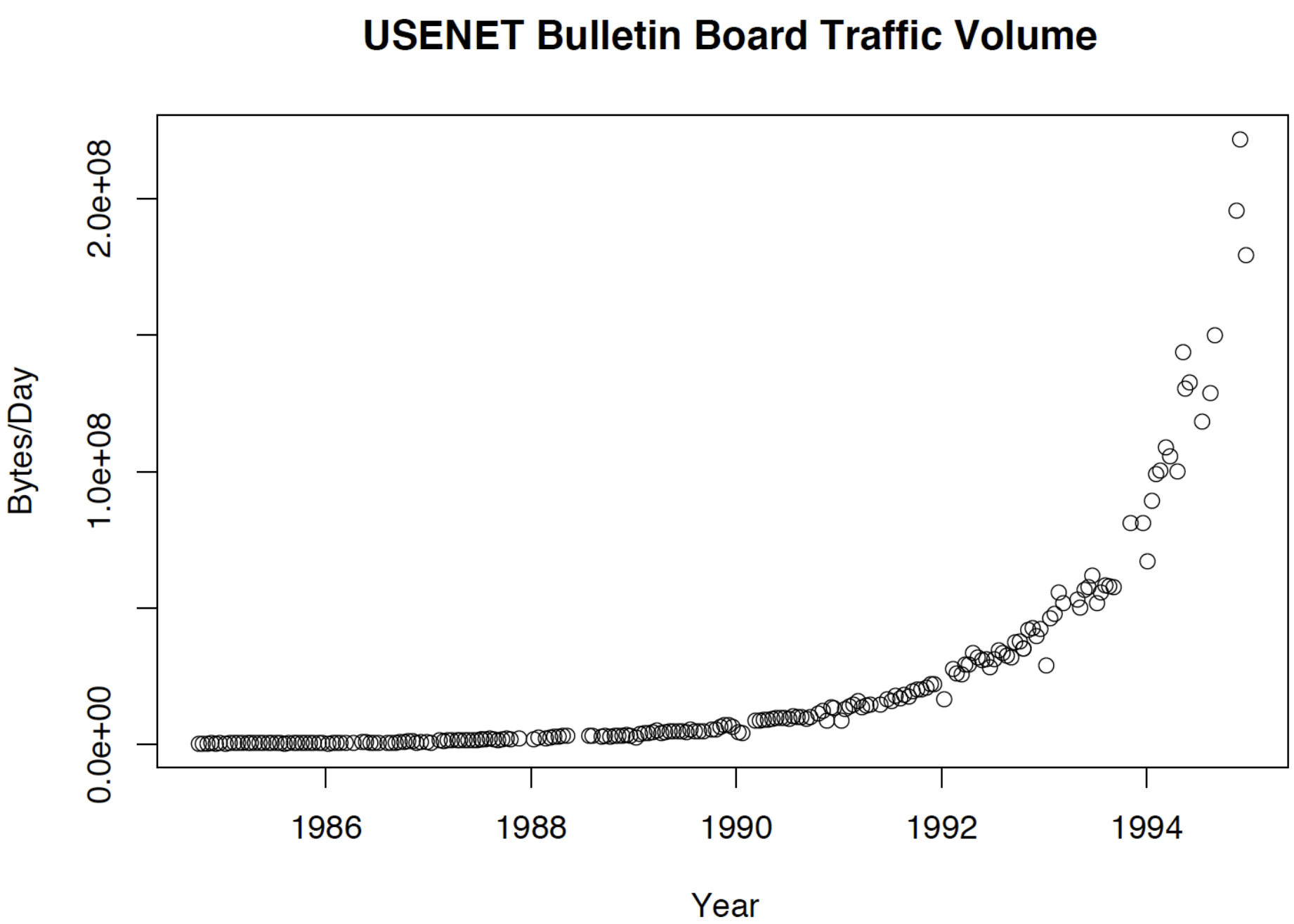
- Jan 5, 1985: Ron Kay discusses the idea of forming ICSI w/ Domenico Ferrari
  - Size of the Internet: ≈ 1,200 hosts
    (340 KB/day through USENET bulletin board system)
- Jun 26, 1986: ICSI incorporated
  - ≈ 3,500 Internet hosts (810 KB/day)
- Jan 1, 1988: Lease at Center Street begins
  - ≈ 29,000 Internet hosts (1.8 MB/day)
- Sep 26, 1988: official inauguration of ICSI
  - 56,000 Internet hosts (3.3 MB/day)

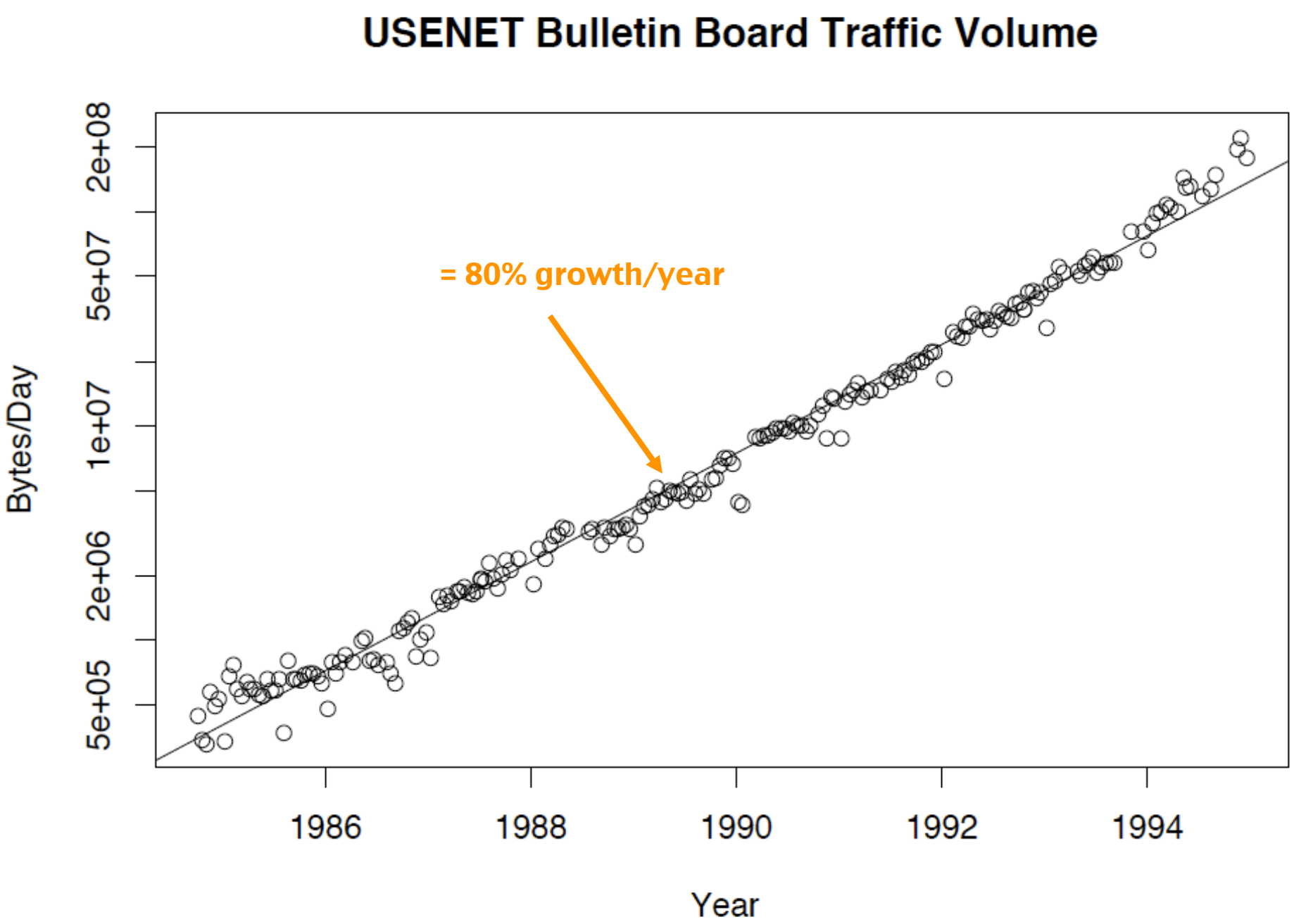
I Start Watching the Internet Develop Too

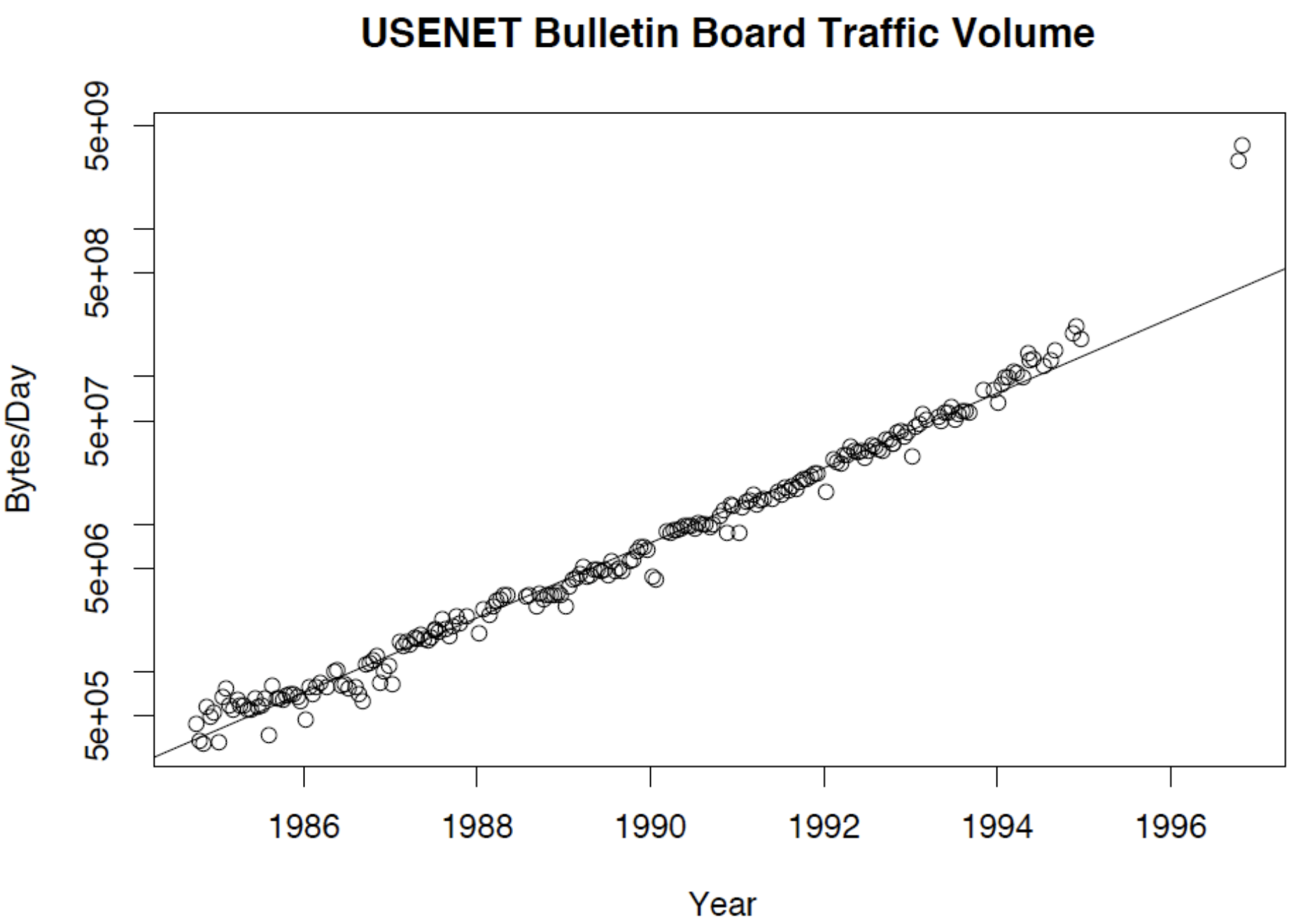
- Sep 1990: I enroll in Prof. Ferrari's grad "special topics" course on networking & start measuring networking traffic at LBL
  - 313,000 Internet hosts (9.5 MB/day)
- Oct 21 1991: I join Prof. Ferrari's *Tenet* group
  - 617,000 Internet hosts (17.5 MB/day)
- May 11, 1994: My 1st paper on network measurement, *Growth Trends in Wide Area TCP Connections*, accepted for publication
  - ≈ 3,000,000 Internet hosts (130 MB/day)

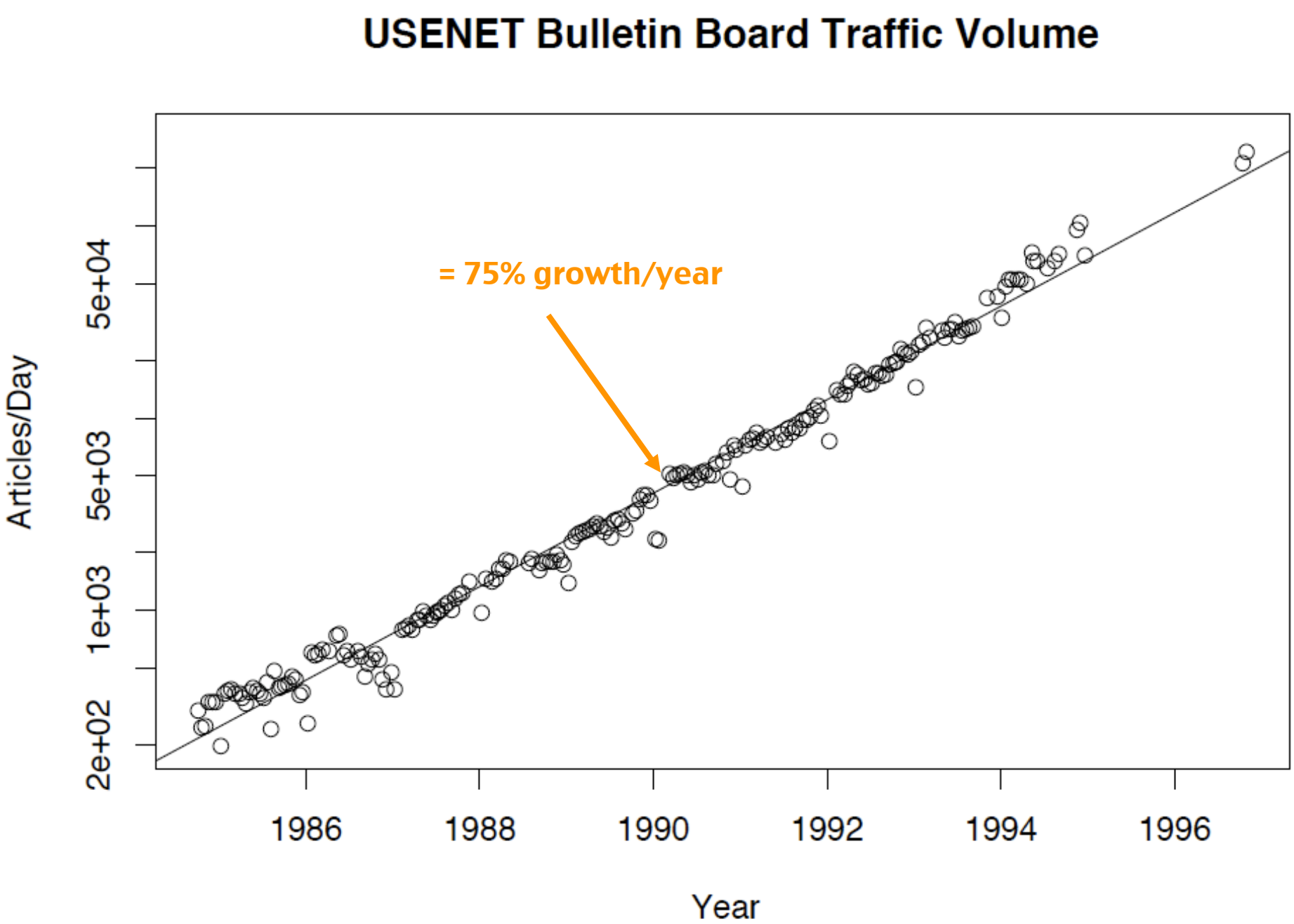


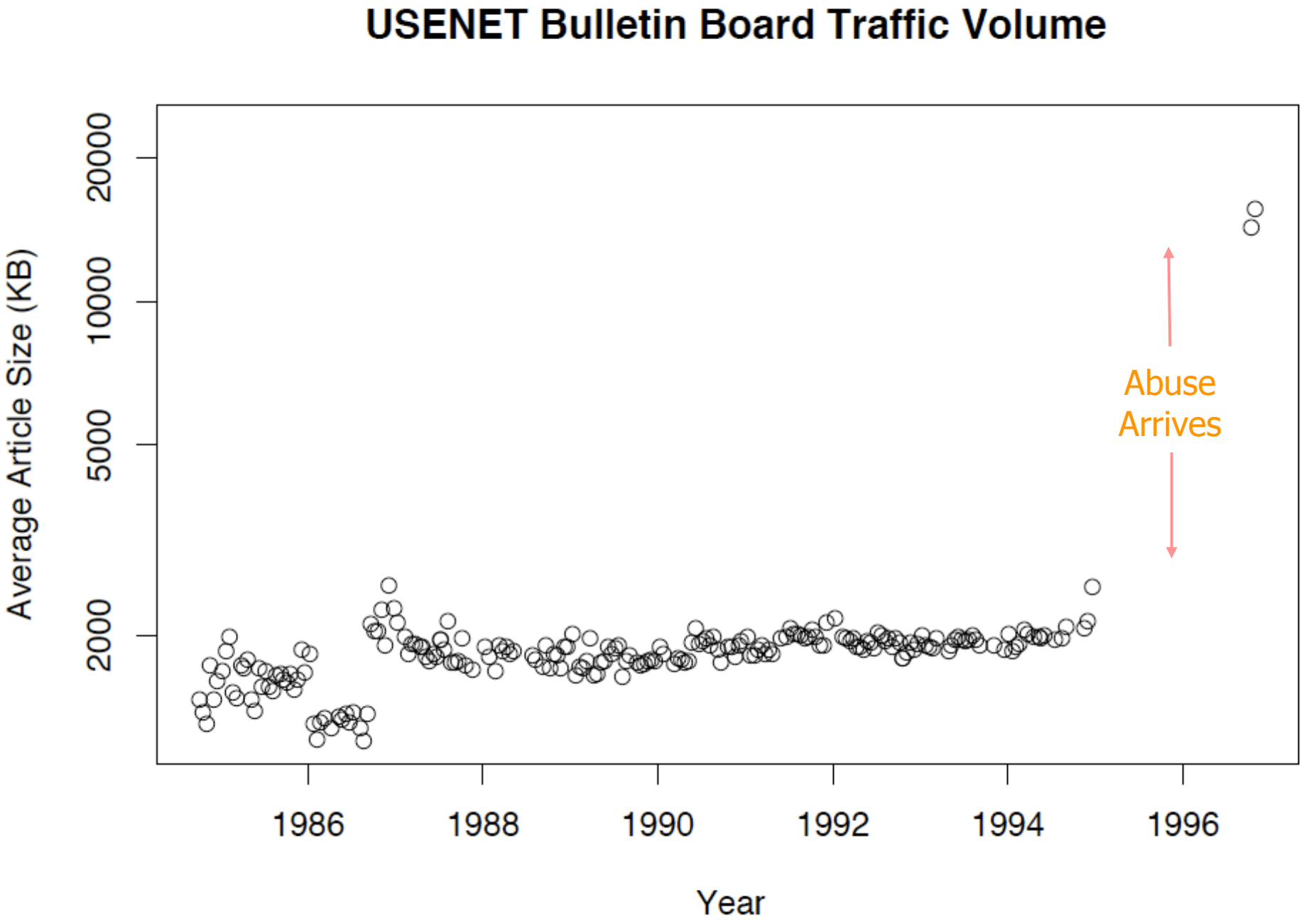
"... relatively new information-retrieval protocols such as Gopher and World-Wide Web exhibited explosive growth"
"Our data suggests a very recent explosion in commercial use of the Internet ..."


USENET Bulletin Board Traffic Volume
Bytes/Day
0.0e+00
1.0e+08
2.0e+08
1986
1988
1990
1992
1994
Year


USENET Bulletin Board Traffic Volume
= 80% growth/year
Bytes/Day
5e+05
2e+06
1e+07
5e+07
2e+08
1986
1988
1990
1992
1994
Year


USENET Bulletin Board Traffic Volume
Bytes/Day
5e+05
5e+06
5e+07
5e+08
5e+09
1986
1988
1990
1992
1994
1996
Year


USENET Bulletin Board Traffic Volume
= 75% growth/year
Articles/Day
2e+02
1e+03
5e+03
5e+04
1986
1988
1990
1992
1994
1996
Year


USENET Bulletin Board Traffic Volume
Average Article Size (KB)
2000
5000
10000
20000
1986
1988
1990
1992
1994
1996
Year
Abuse
Arrives

Mid-1990s: Internet Abuse Starts Becoming a Concern

- Observation: operators increasingly ask whether network data sheds light on security incidents
  - Hmmm, what about doing such measurement purposefully for security monitoring?
- Armed with equipment donation from DEC, the Bro *intrusion detection system* starts operating 24x7 in 1996
  - Inspects LBL border traffic in real-time
  - Who-talks-to-whom, what service, how much data
  - And, increasingly: what are the **semantics** of the conversations

Detecting Attackers, 1990s-style

- Inspect access to sensitive objects:
  - Hosts, usernames (“`lp`”, “`r00t`”), filenames (“`/etc/passwd`”), services (“`mountd`”, Windows file sharing)
- Look for specific forms of protocol abuse
  - E.g., FTP “`site exec`”, excessively long “`finger`” requests
- Check for telling behavior
  - Local host starts running an IRC chat server
  - Outbound requests to `www.uberhax0r.net`, `anticode.com`
  - Login sessions containing: “`unset histfile`”; “`eggdrop`”; “`printf(“overflowing”`; “`smurf.c by Tfreak`”; “`Super Linux Xploit`”; “`Coded by James Seter`”
- Attackers exploit systems via interactive login sessions
  - Motivated by bragging rights / vandalism
  - Frequent community reuse of tools
  - Employment of “bots” for automating IRC management
- But what about “serious” attackers rather than weenies?

Real-World Security: *Threat Model*

- 1990s academic computer security research heavily influenced by cryptography's standard of mathematical assessment of security strength
  - Prove security properties …
  - … given a model of a powerful adversary
- In practice, goal is risk management, not bulletproof protection.
  - Much of the effort concerns "raising the bar" and *trading off resources*
- Threat model: what you are defending against
  - This can differ from what an academic might expect
  - Consider the Department of Energy …

MANUAL

DOE M 470.4-1

Approved: 8-26-05
Review: 8-26-07
Chg 1: 3-7-06

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

U.S. DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

Vertical line denotes change.

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		

Department of Energy
Washington, DC 20585

August 7, 2006

MEMORANDUM FOR: ASSOCIATE DIRECTORS
OFFICE DIRECTORS
SITE OFFICE MANAGERS

FROM: GEORGE MALOSH
ACTING CHIEF OPERATING OFFICER
OFFICE OF SCIENCE

SUBJECT: Office of Science Policy on the Protection of Personally Identifiable Information

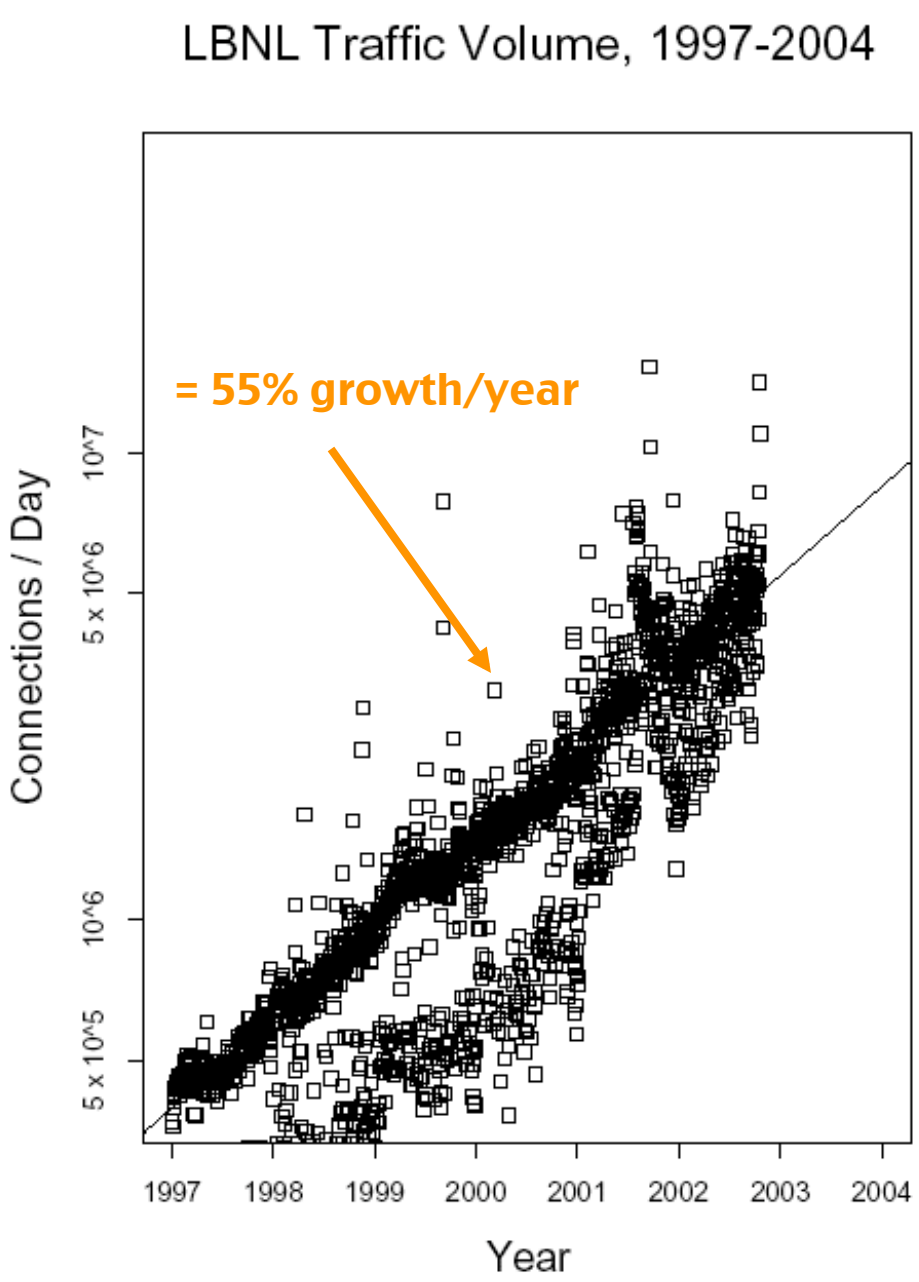
The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing

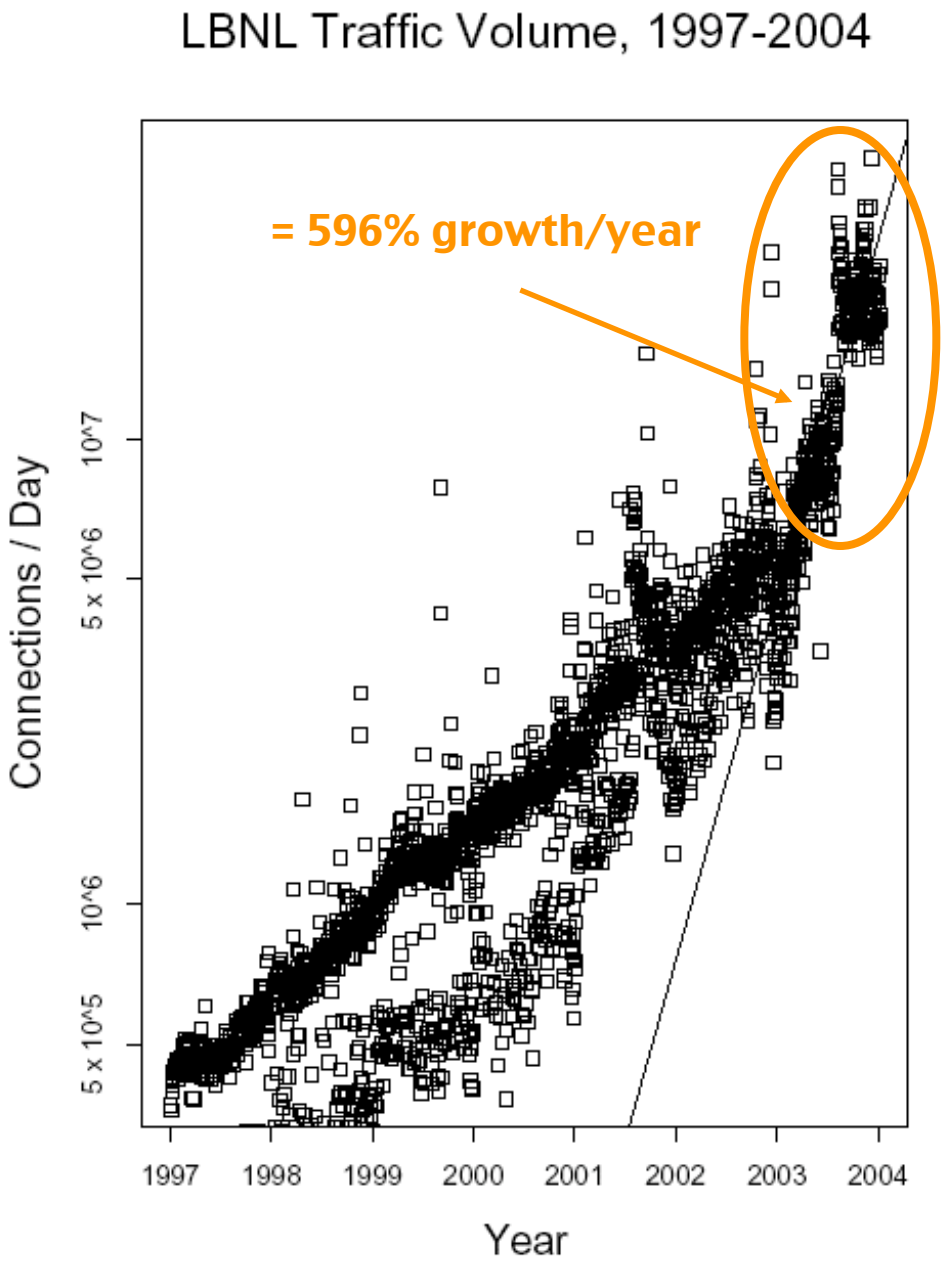
- **Incident Reporting**

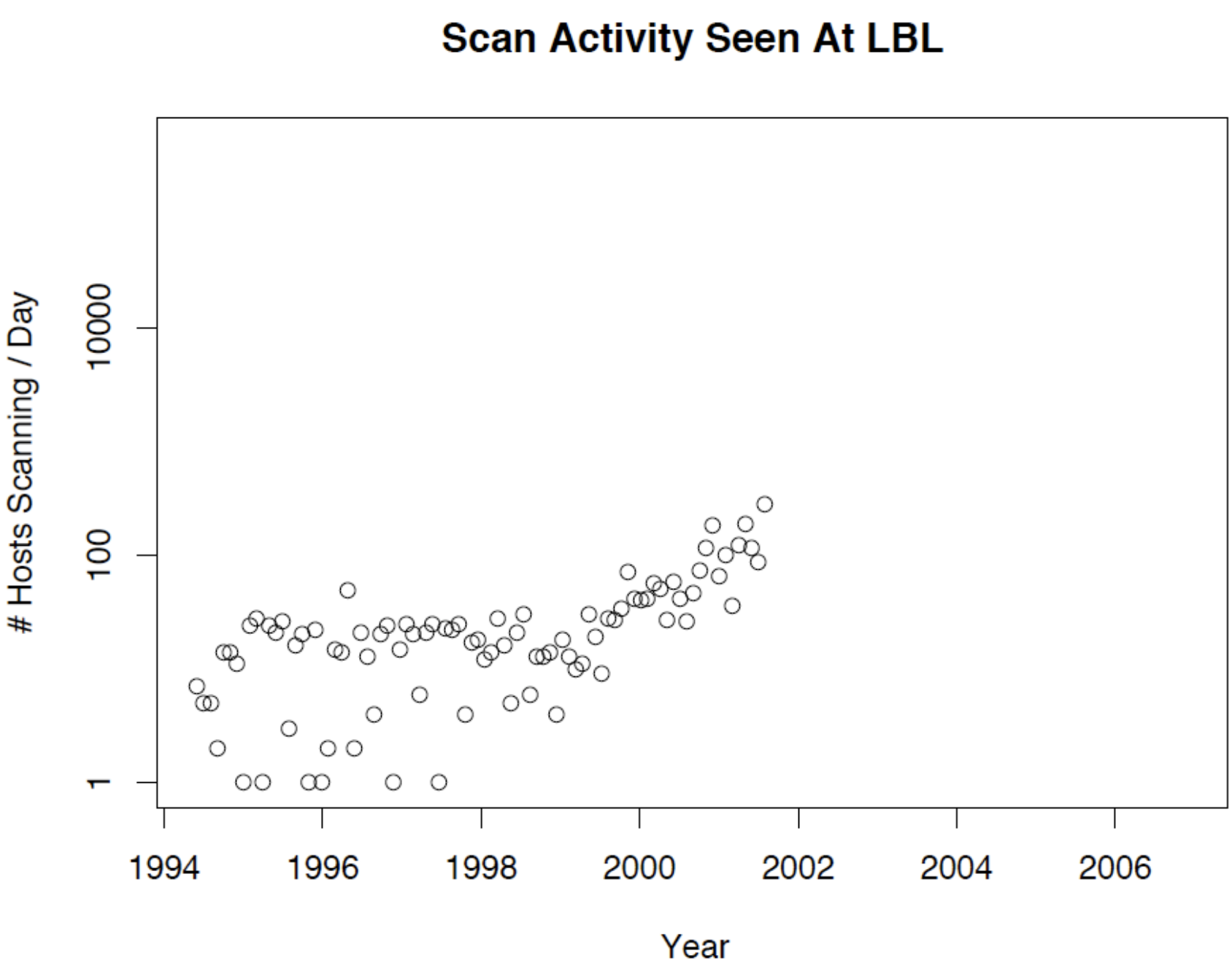
Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

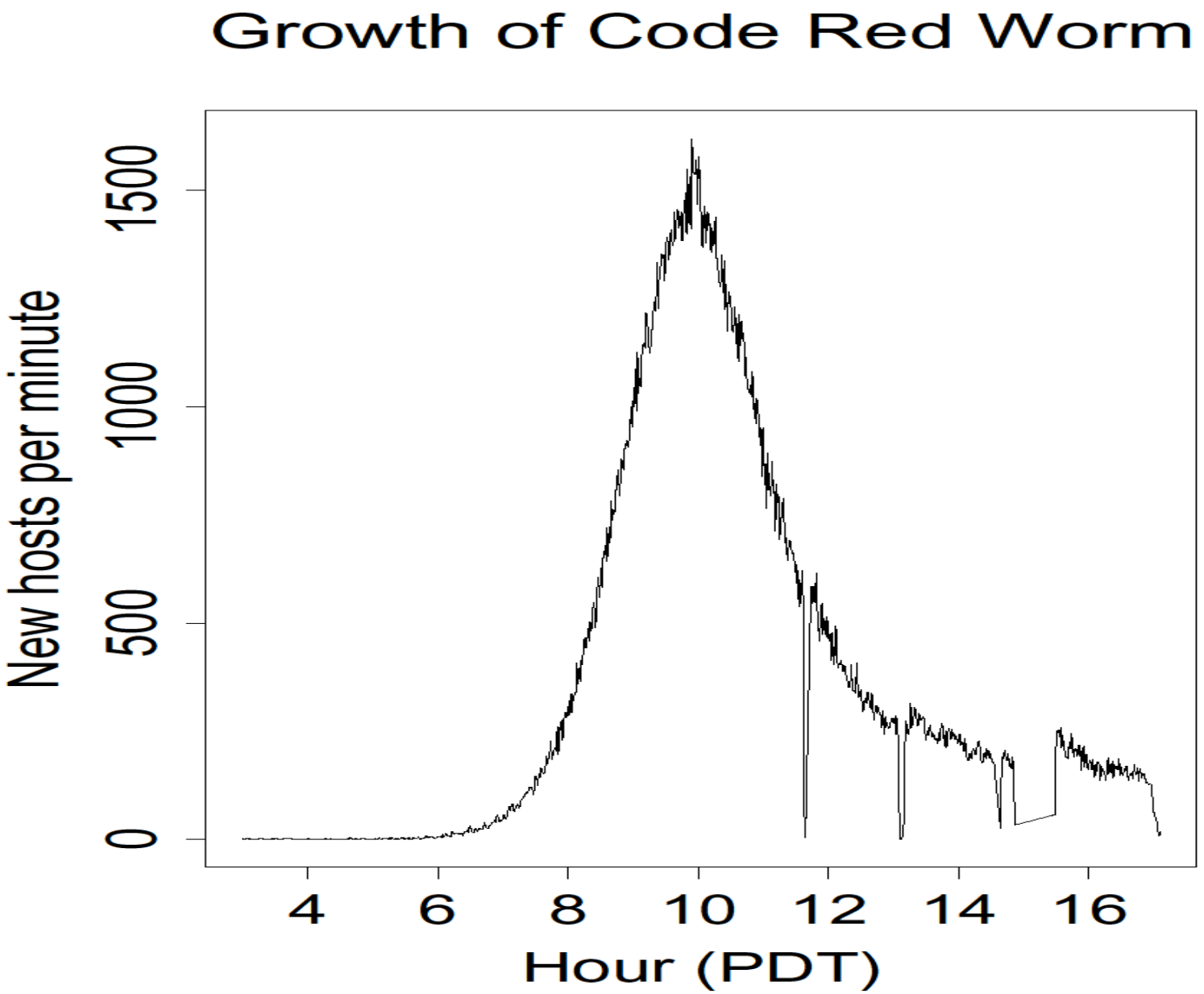
Network Security Research Grounded in Operational Use

- Our ties with LBL operational deployment have been **research gold**
  - *Transformative* compared to working in small, self-contained environment like a lab
- Along with *threat model* (policy) realities, **scale** completely alters the problem landscape:
  - Performance - current target: analyze >> 100K pps
    - Research on: clustering; FPGA front end; multicore architecture
  - Diversity - you see the darnedest (benign) "crud"
    - Greatly complicates **anomaly detection** & detecting **evasion**
  - Base Rate Fallacy - detector w/ 10^{-6} error rate might not work!
- Another operational reality: intrusion **prevention**
  - Bro enabled to *automatically block* LBL traffic
    - Very high standard for accuracy!
  - #1 gain: dropping *scanners*


LBNL Traffic Volume, 1997-2004
= 55% growth/year
Connections / Day
5 x 10^5
10^6
5 x 10^6
10^7
1997
1998
1999
2000
2001
2002
2003
2004
Year


LBNL Traffic Volume, 1997-2004
= 596% growth/year
Connections / Day
5 x 10^5
10^6
5 x 10^6
10^7
1997
1998
1999
2000
2001
2002
2003
2004
Year


Scan Activity Seen At LBL
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year

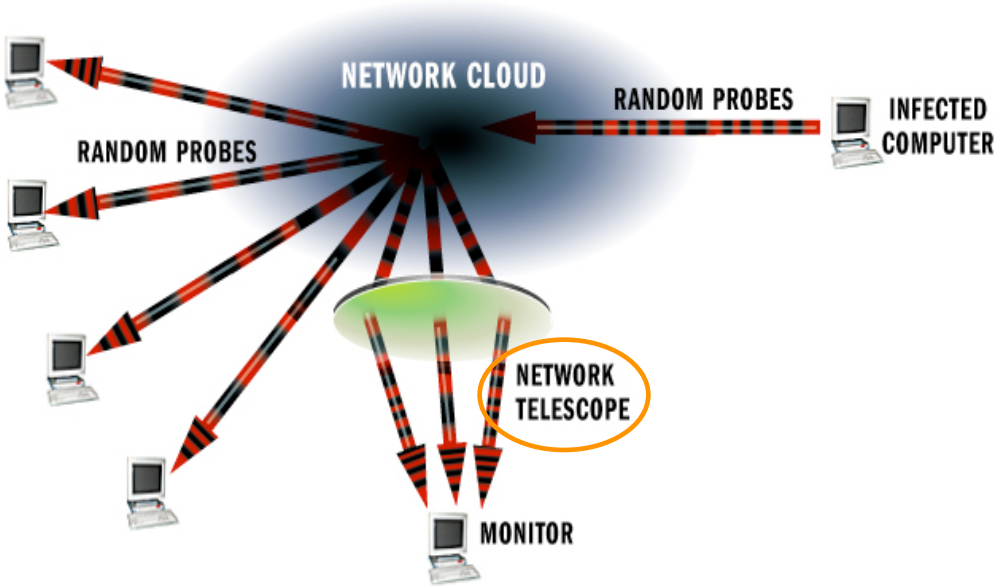

Growth of Code Red Worm
New hosts per minute
0
500
1000
1500
4
6
8
10
12
14
16
Hour (PDT)

Worms

- When attacker compromises a host, they can instruct it to do whatever they want
- Automatically instructing it to find *more* vulnerable hosts to repeat the process creates a **worm**: a program that self-replicates across a network
  - Often spread by picking 32-bit Internet addresses at random to probe …
- As worm repeatedly replicates, it grows *exponentially fast*
  - Each copy of the worm works **in parallel** to find more victims
- Can be **big** and **fast** …
  - Code Red (2001): 369K, 10 hours
  - Blaster (2003), 9M, 9 days (25M+ total)
  - Slammer (2003), 75K, < 10 min
  - Our paper designs (2004): 1M in ≈ 2 sec
  - Or: $50-150B damage in 1 day

Worm Detection

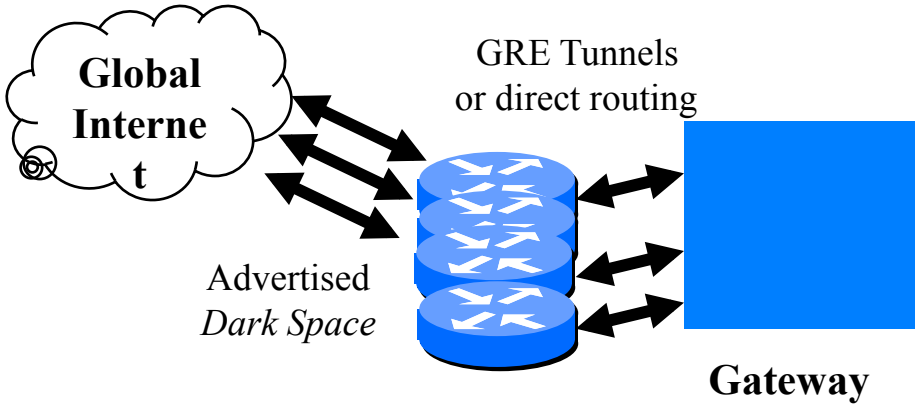
- Particular problem: detect a new global outbreak very quickly and very accurately.
- Key notion: given random scanning by worms, if we monitor a large number of addresses, they will come to us

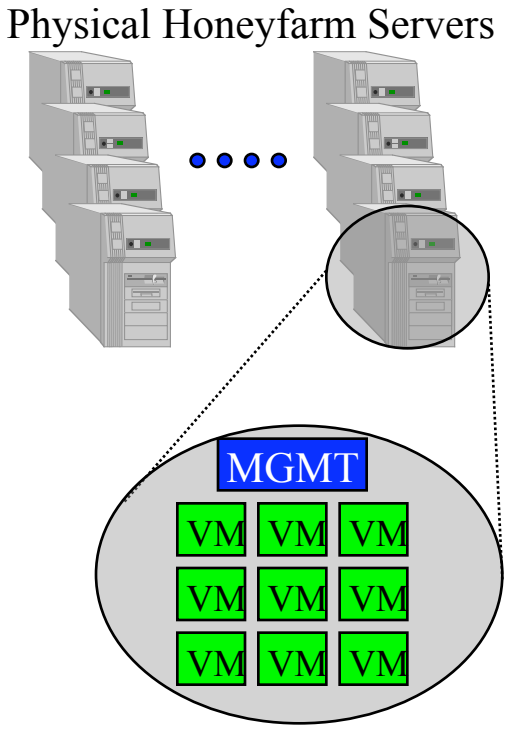


*Pursued as a **CCIED** Effort: Collaborative Center for Internet Epidemiology & Defenses (w/ UCSD)*

GQ: Building a Large-Scale *Honeyfarm*

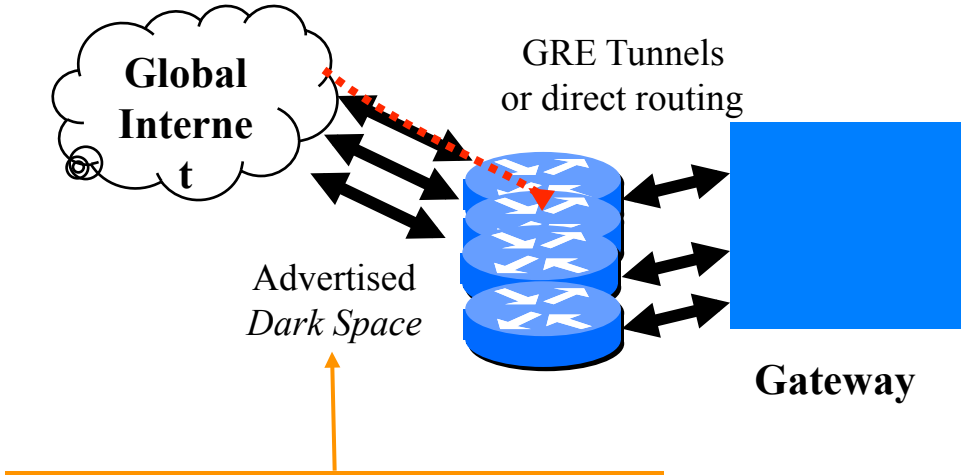
- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity



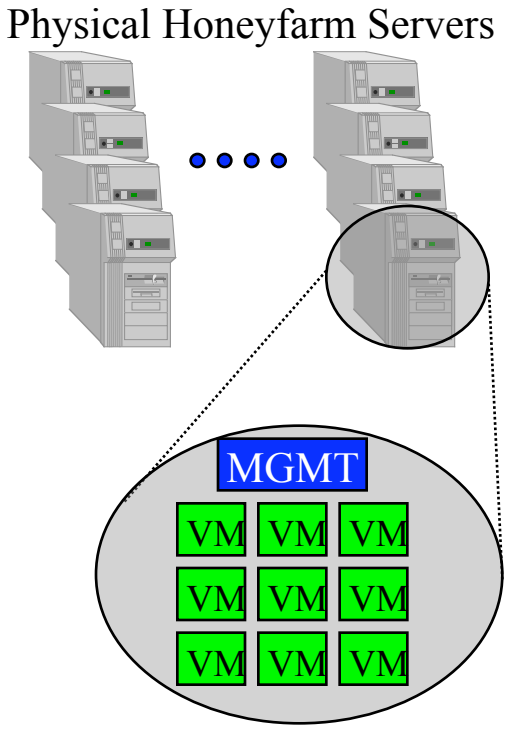


GQ: Building a Large-Scale *Honeyfarm*

- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity

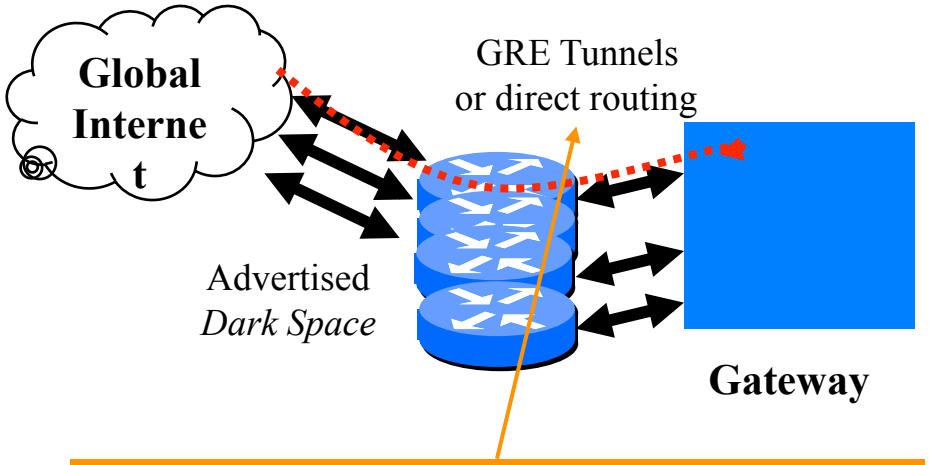


Dark space: blocks of otherwise unallocated addresses

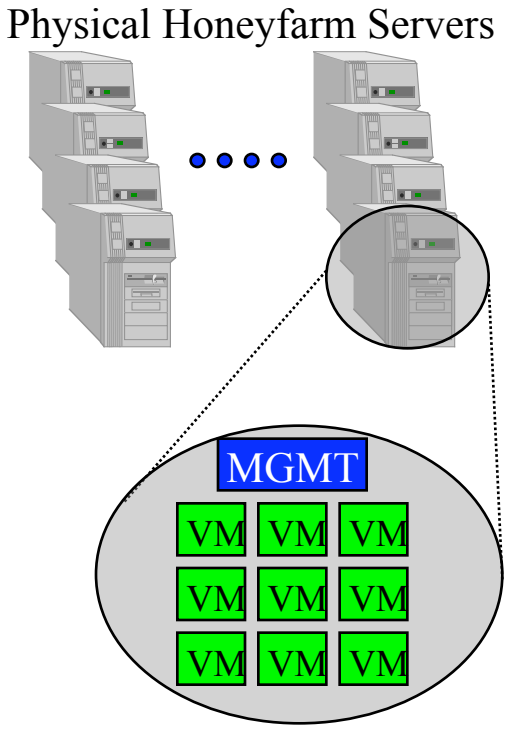


GQ: Building a Large-Scale *Honeyfarm*

- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity

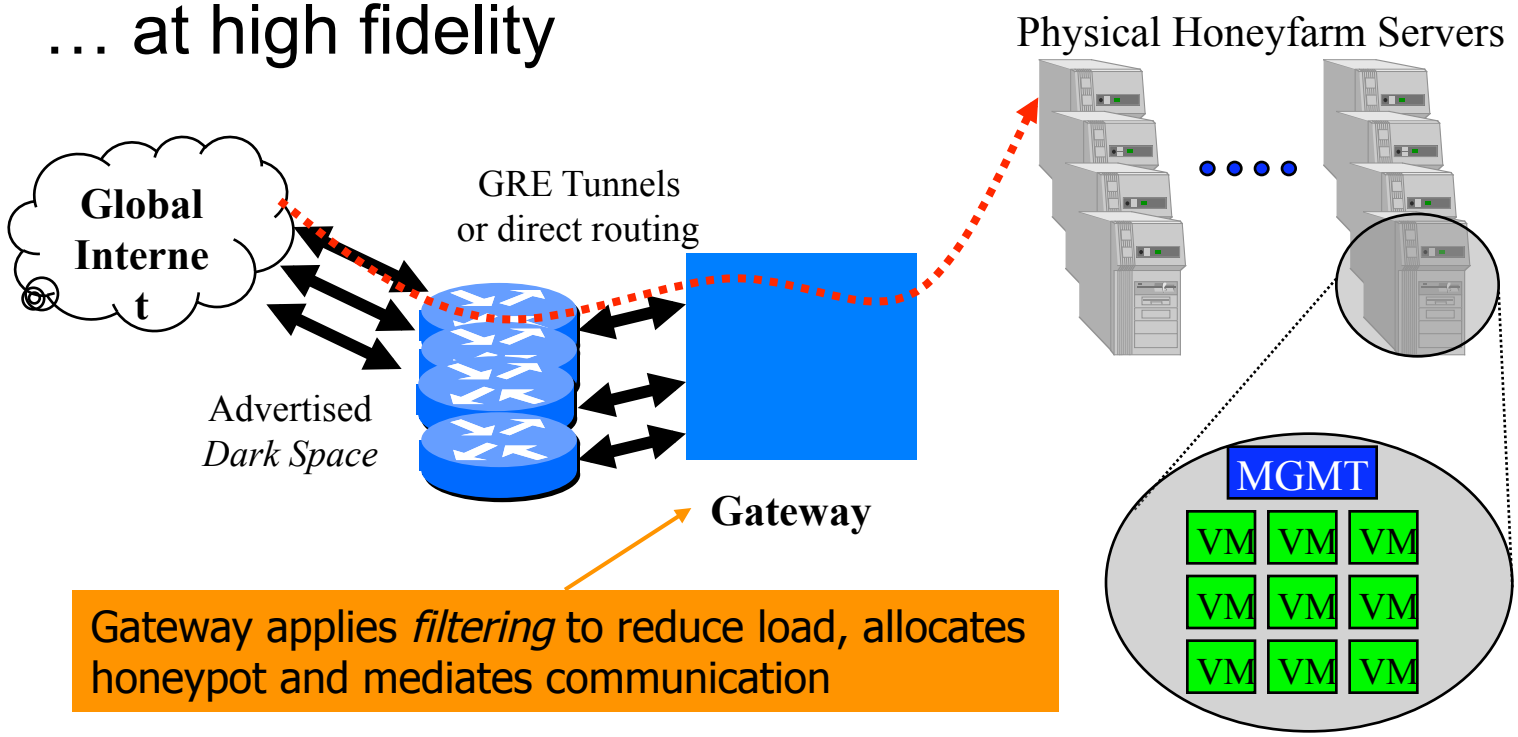


Routers send dark space traffic either via tunnels or direct attachment



GQ: Building a Large-Scale *Honeyfarm*

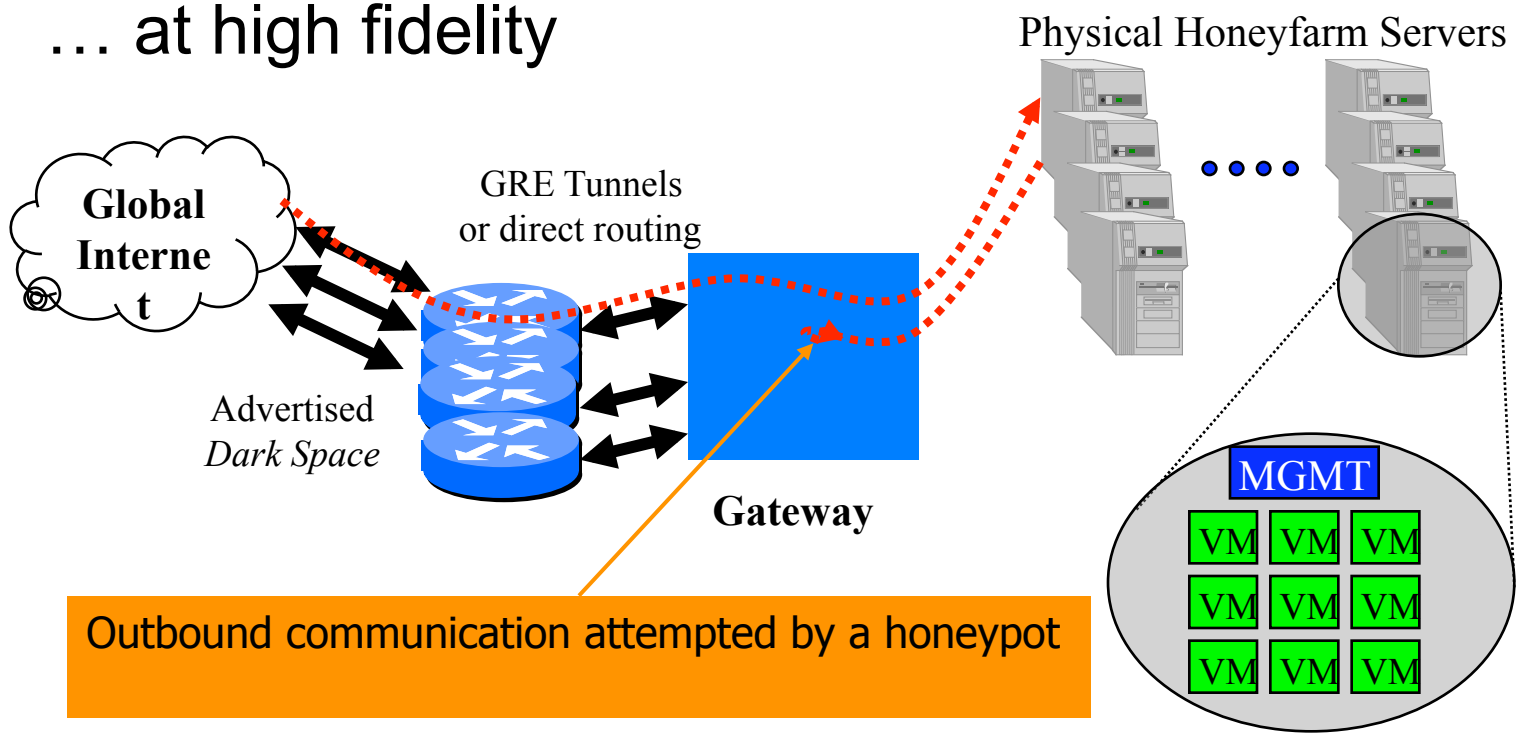
- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity



Gateway applies *filtering* to reduce load, allocates honeypot and mediates communication

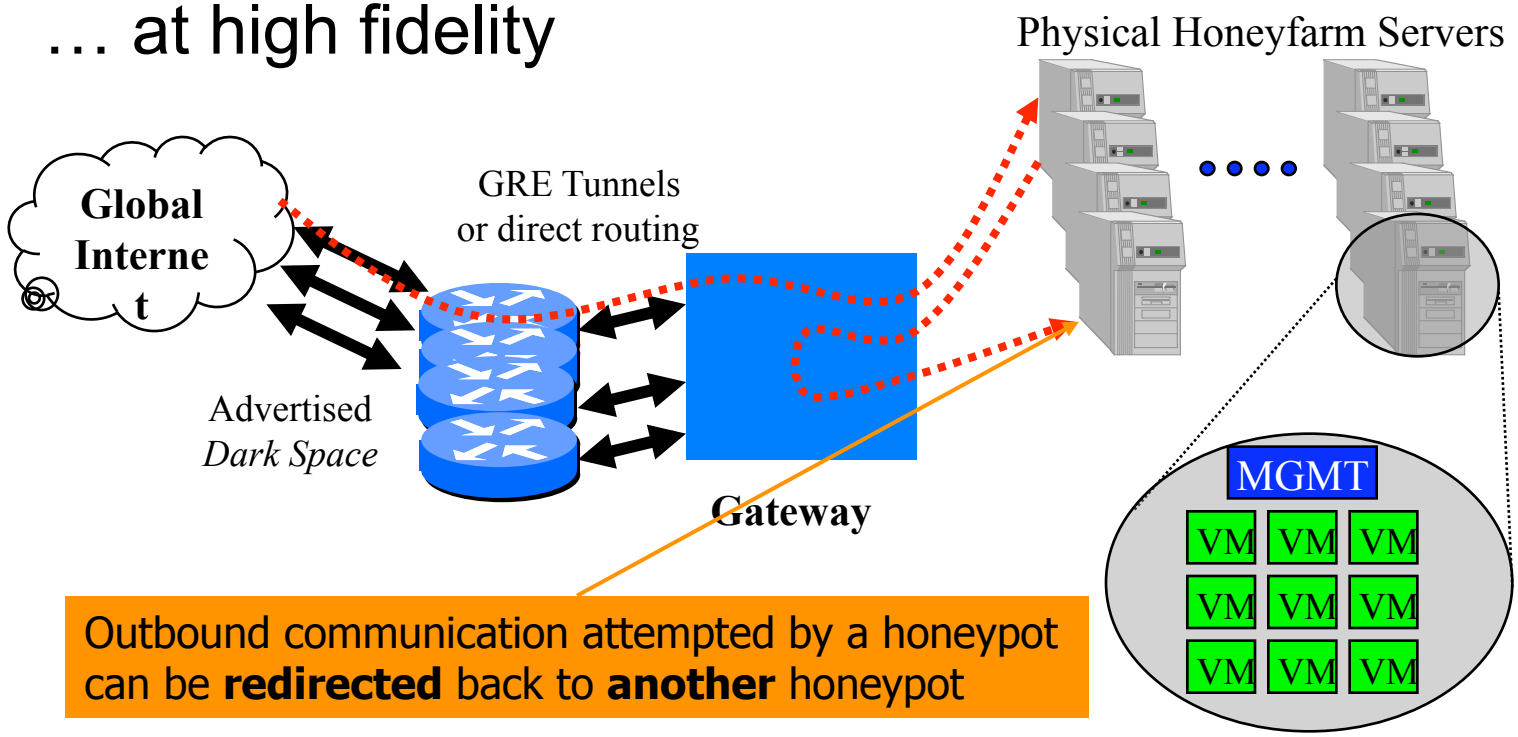
GQ: Building a Large-Scale *Honeyfarm*

- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity



GQ: Building a Large-Scale *Honeyfarm*

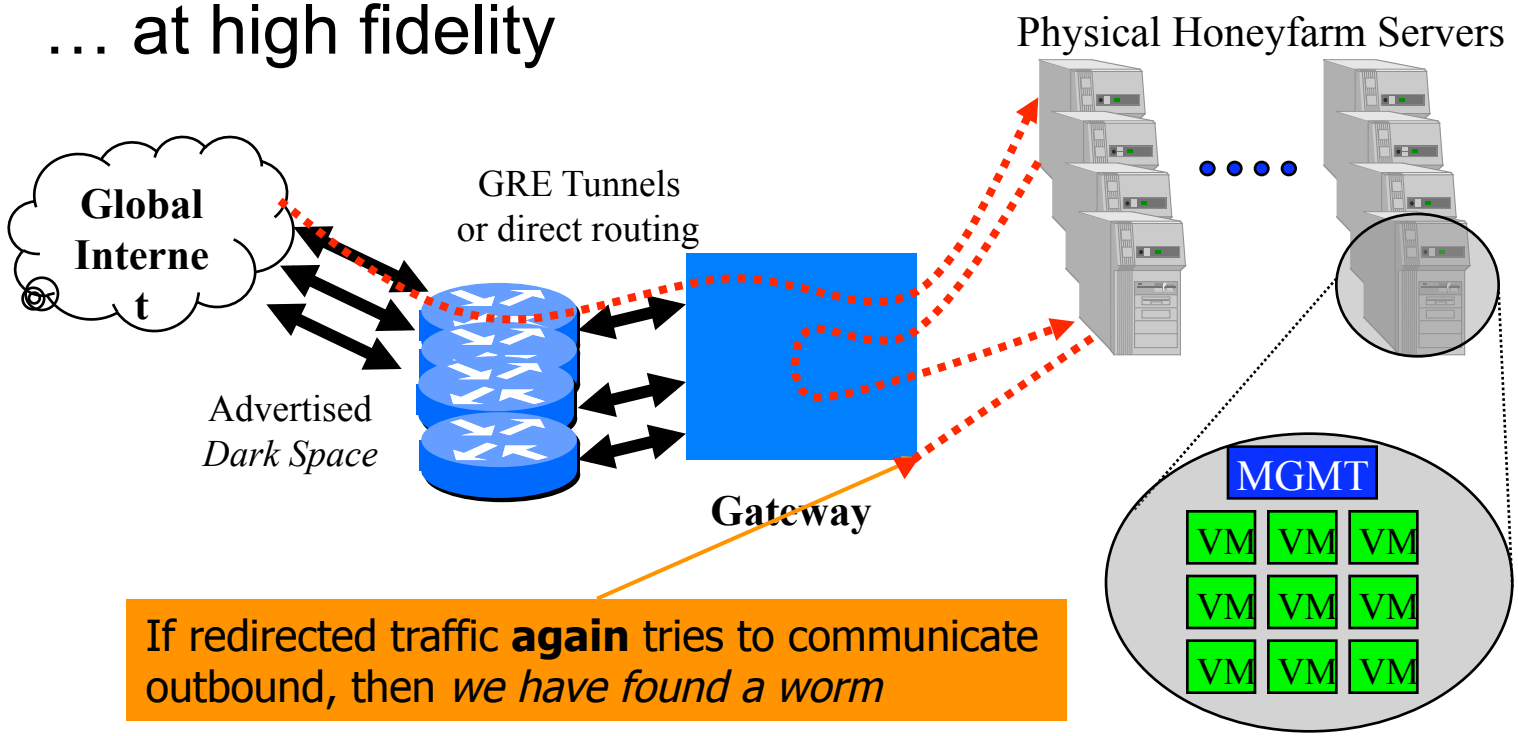
- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity



Outbound communication attempted by a honeypot can be **redirected** back to **another** honeypot

GQ: Building a Large-Scale *Honeyfarm*

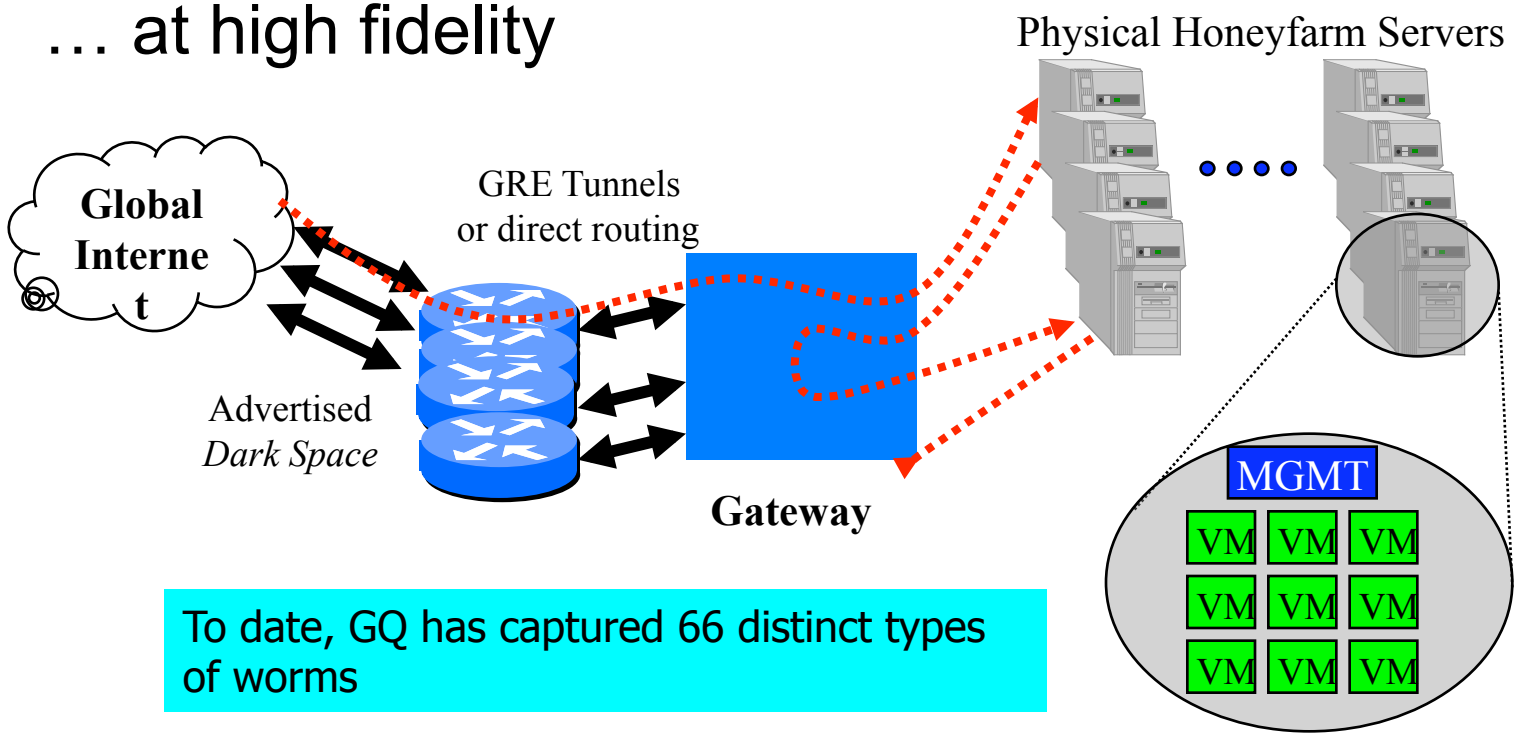
- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity



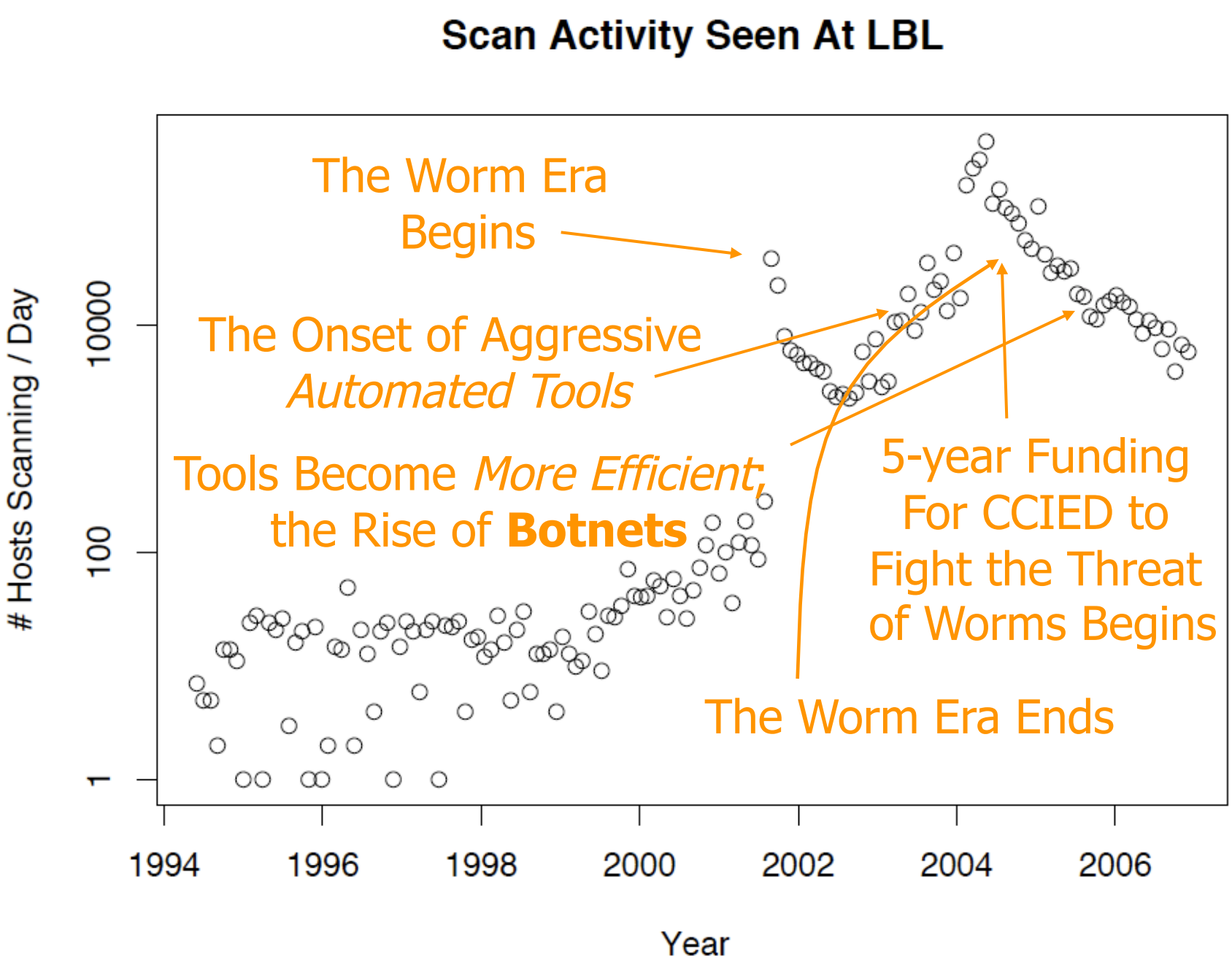
If redirected traffic **again** tries to communicate outbound, then *we have found a worm*

GQ: Building a Large-Scale *Honeyfarm*

- *Honeyfarm*: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 250,000+ monitored addresses …
- … at high fidelity

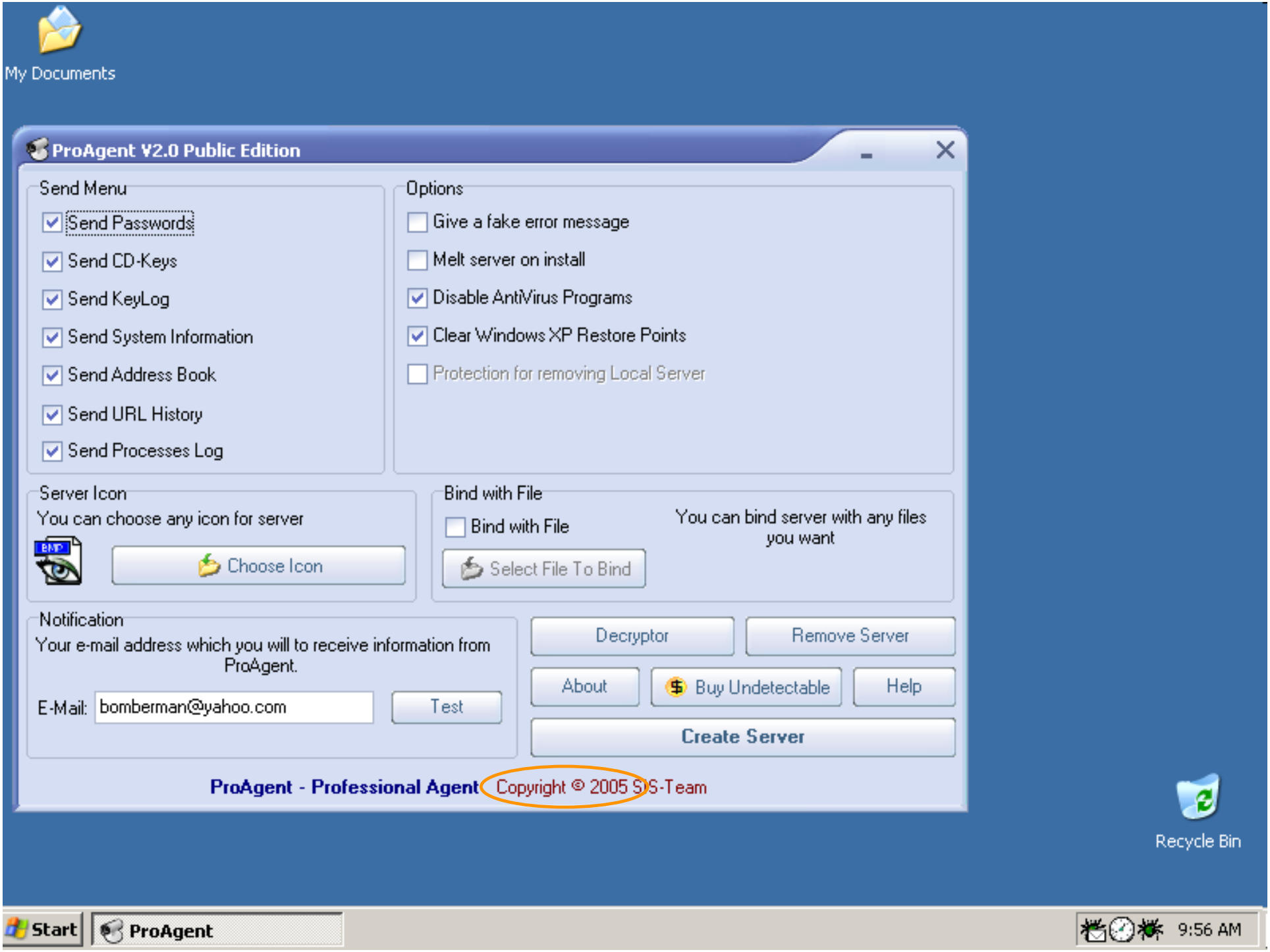


To date, GQ has captured 66 distinct types of worms


Scan Activity Seen At LBL
The Worm Era Begins
The Onset of Aggressive Automated Tools
Tools Become More Efficient; the Rise of Botnets
5-year Funding For CCIED to Fight the Threat of Worms Begins
The Worm Era Ends
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year

Part II

Selling Viagra®


My Documents
ProAgent ¥2.0 Public Edition
Send Menu
Send Passwords
Send CD-Keys
Send KeyLog
Send System Information
Send Address Book
Send URL History
Send Processes Log
Options
Give a fake error message
Melt server on install
Disable AntiVirus Programs
Clear Windows XP Restore Points
Protection for removing Local Server
Server Icon
You can choose any icon for server
Choose Icon
Bind with File
Bind with File
You can bind server with any files you want
Select File To Bind
Notification
Your e-mail address which you will to receive information from ProAgent.
E-Mail: bomberman@yahoo.com
Test
Decryptor
Remove Server
About
Buy Undetectable
Help
Create Server
ProAgent - Professional Agent
Copyright © 2005 SIS-Team
Recycle Bin
Start
ProAgent
9:56 AM

Spy Instructors Software

NEW GENERATION SOFTWARE SOLUTIONS

HOMEPAGE | PRODUCTS | DOWNLOADS | FORUMS | ABOUT US

ProAgent v2.1

- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.
- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!
- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!
- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

SIS - Products

Purchase Program

Customer Support Department

Commercial Programs

Freeware Programs

Custom Special Programs

New Generation Software Solutions...

New Products

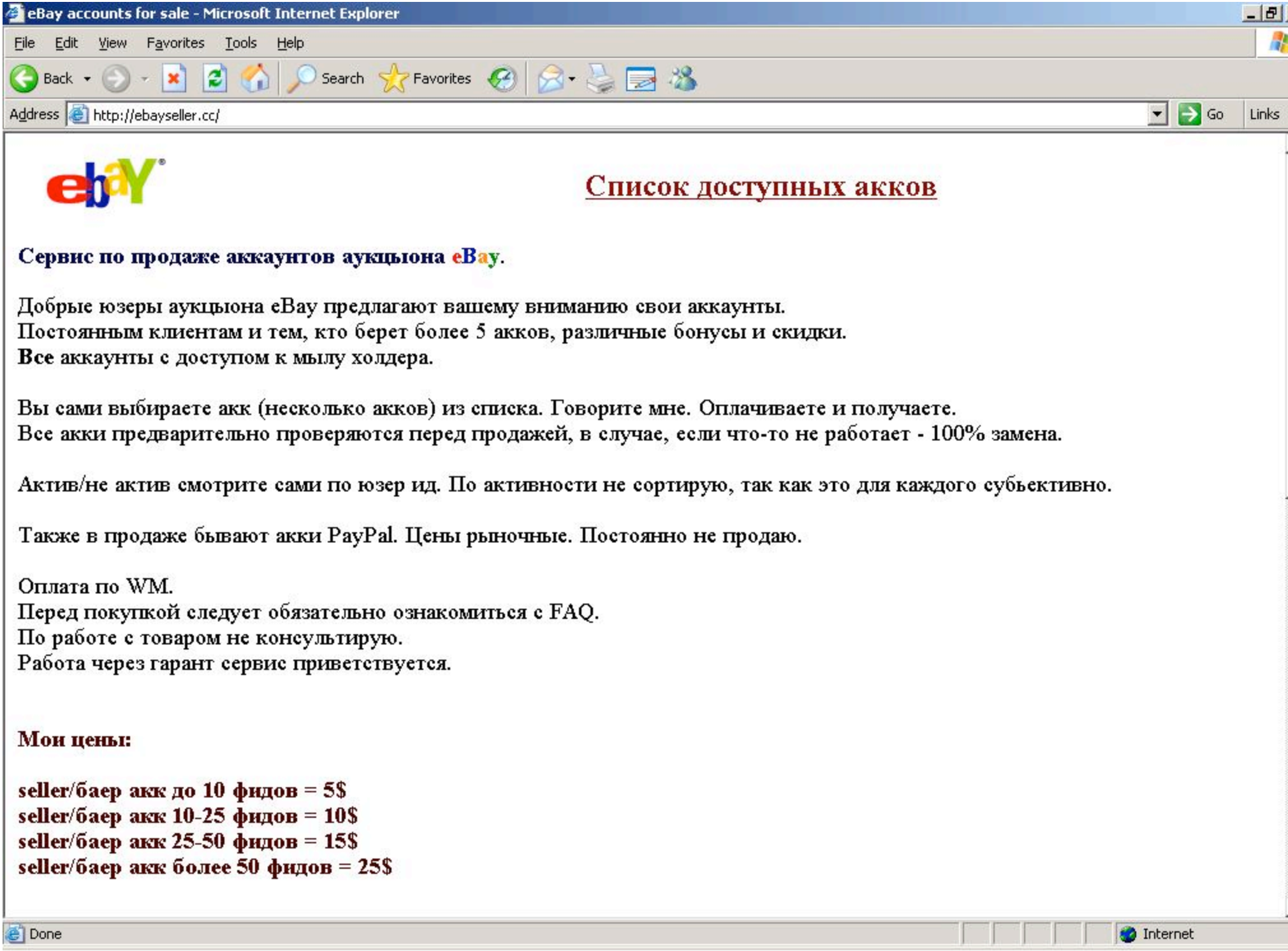
SIS-IExploiter v2.0

ProAgent v2.1

AntiDote v1.2

SIS-Downloader

Virtual Keyboard


eBay accounts for sale - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ebayseller.cc/
Go Links
Список доступных акков
Сервис по продаже аккаунтов аукцыона eBay.
Добрые юзеры аукцыона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.
Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.
Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.
Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.
Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.
Мои цены:
seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$
Done
Internet

allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypasser**** in all of our bots.

Winsock (Multi-threaded) Bots

Become an **Affiliate** and **Start Earning Now**

Click here for 30+ MySpace Bots

Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

Social Networks

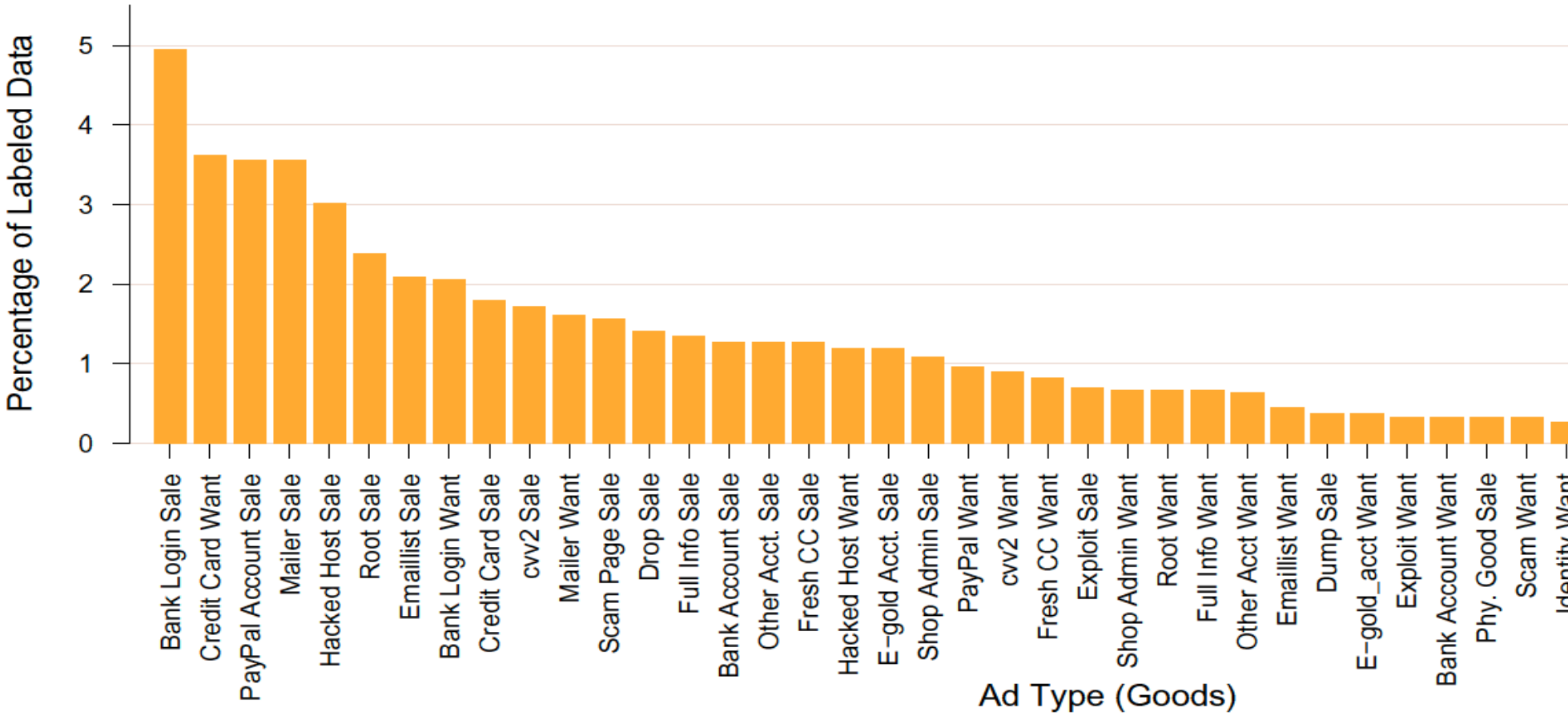
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	PayPal Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager **(Winsock)**	PayPal Buy Now	~~$360.95~~	$320.00
YouTube Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Friendster Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
Hi5 Accounts Creator	PayPal Buy Now	~~$120.95~~	$95.00
TagWorld Accounts Creator	PayPal		

Friend Adders, Message Senders, Comment Posters & Others

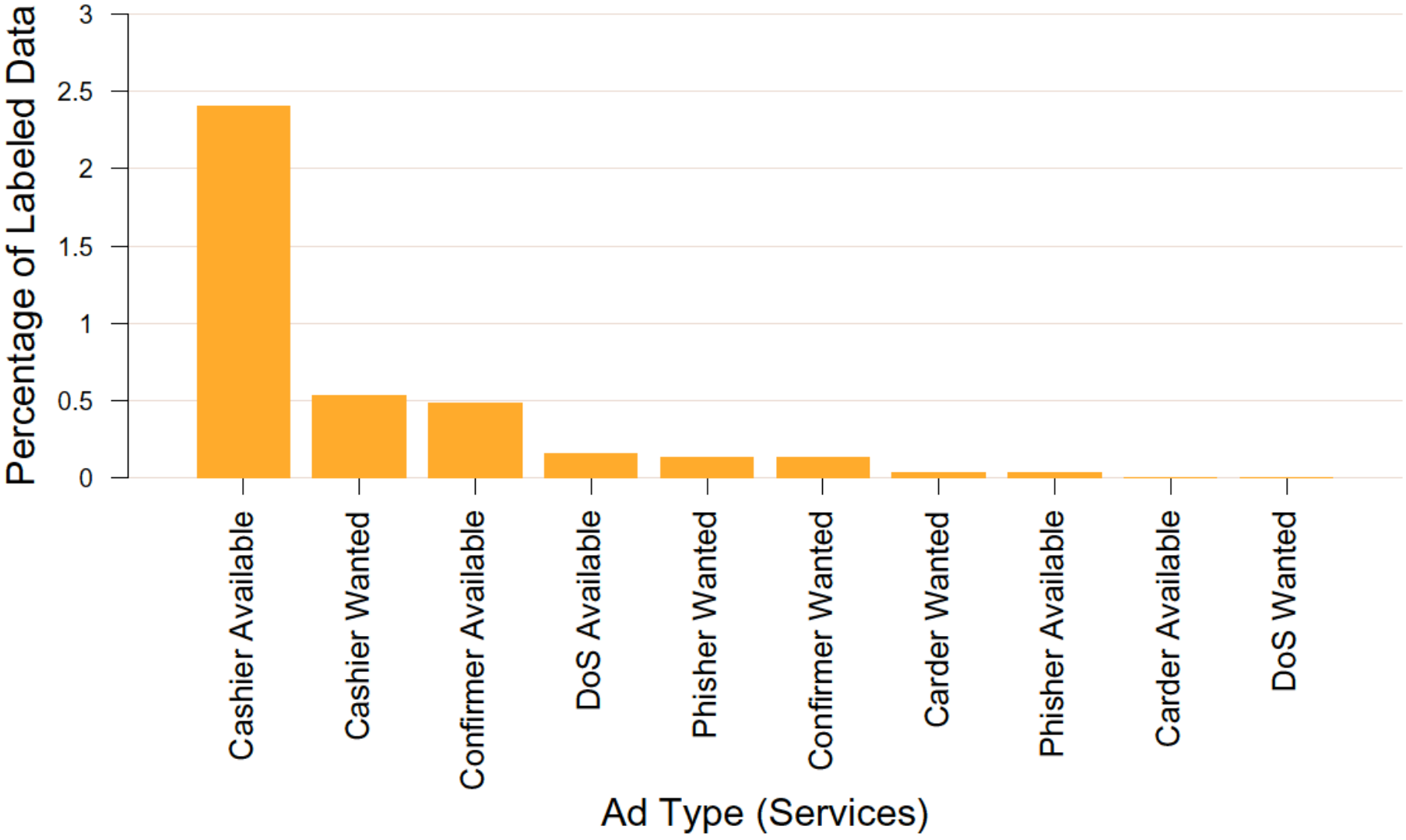
(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

Chaining Feature Is Available On All Bots for All Networks Except Facebook

Marketplace Ads for Goods

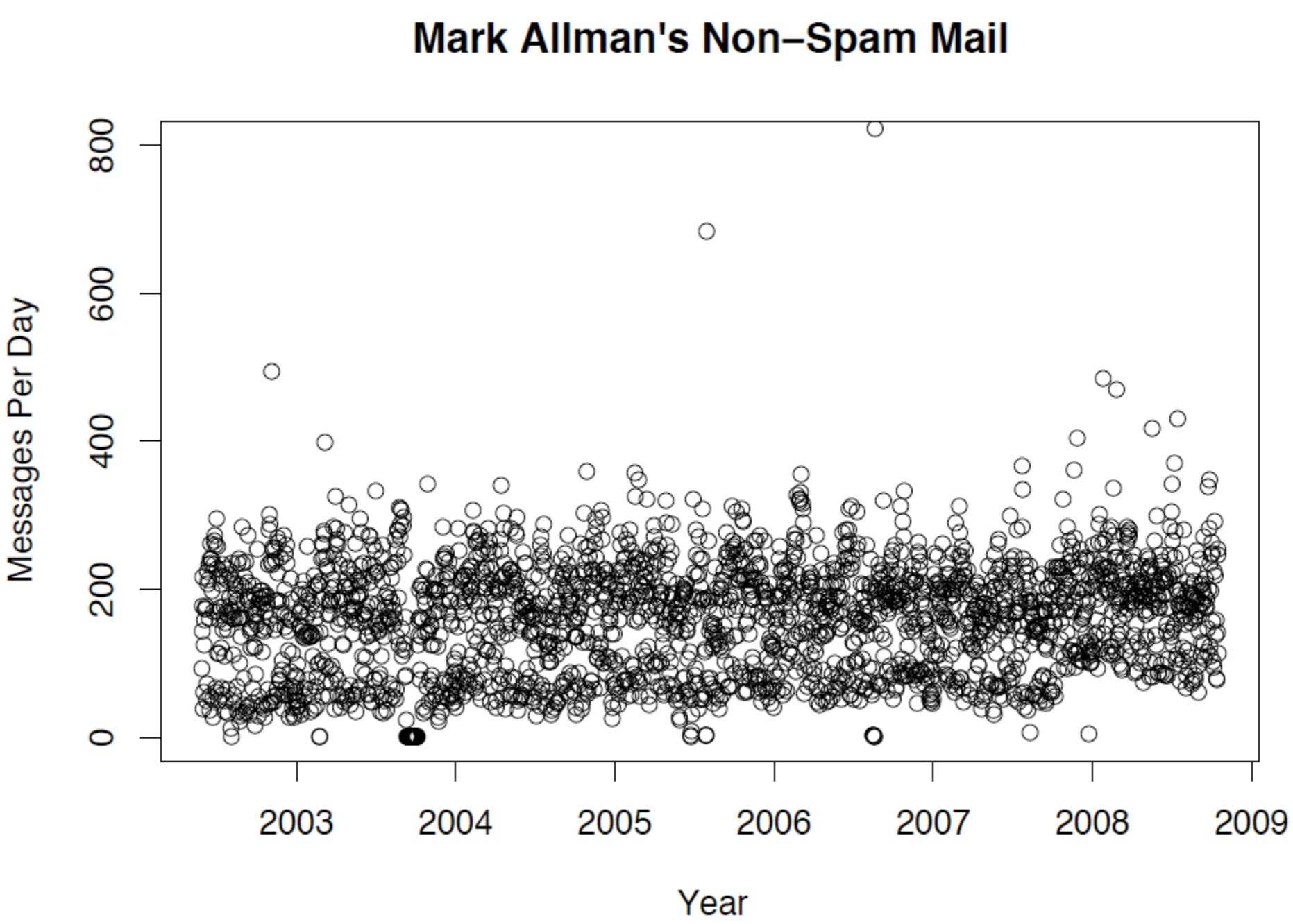


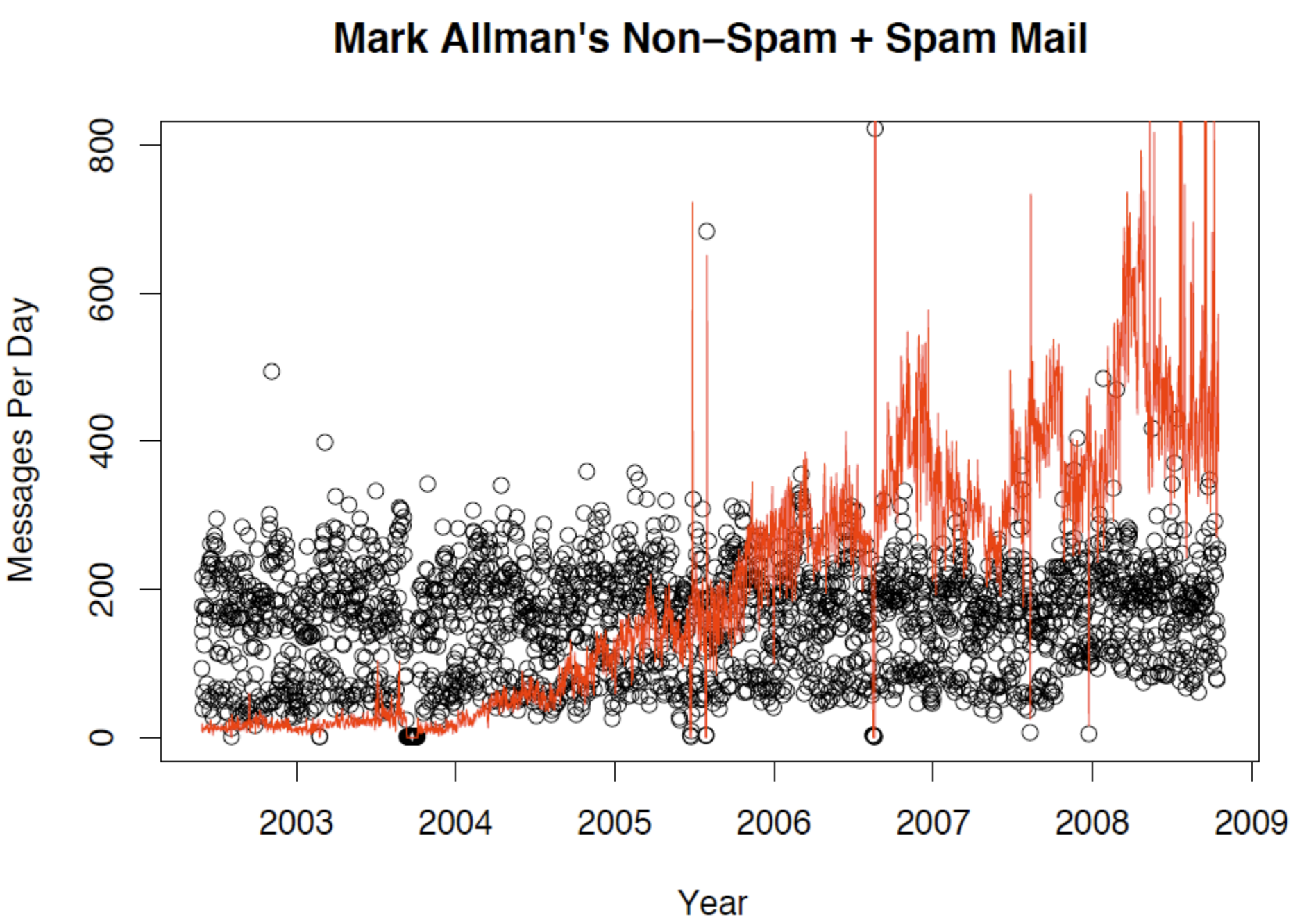
Marketplace Ads for Services

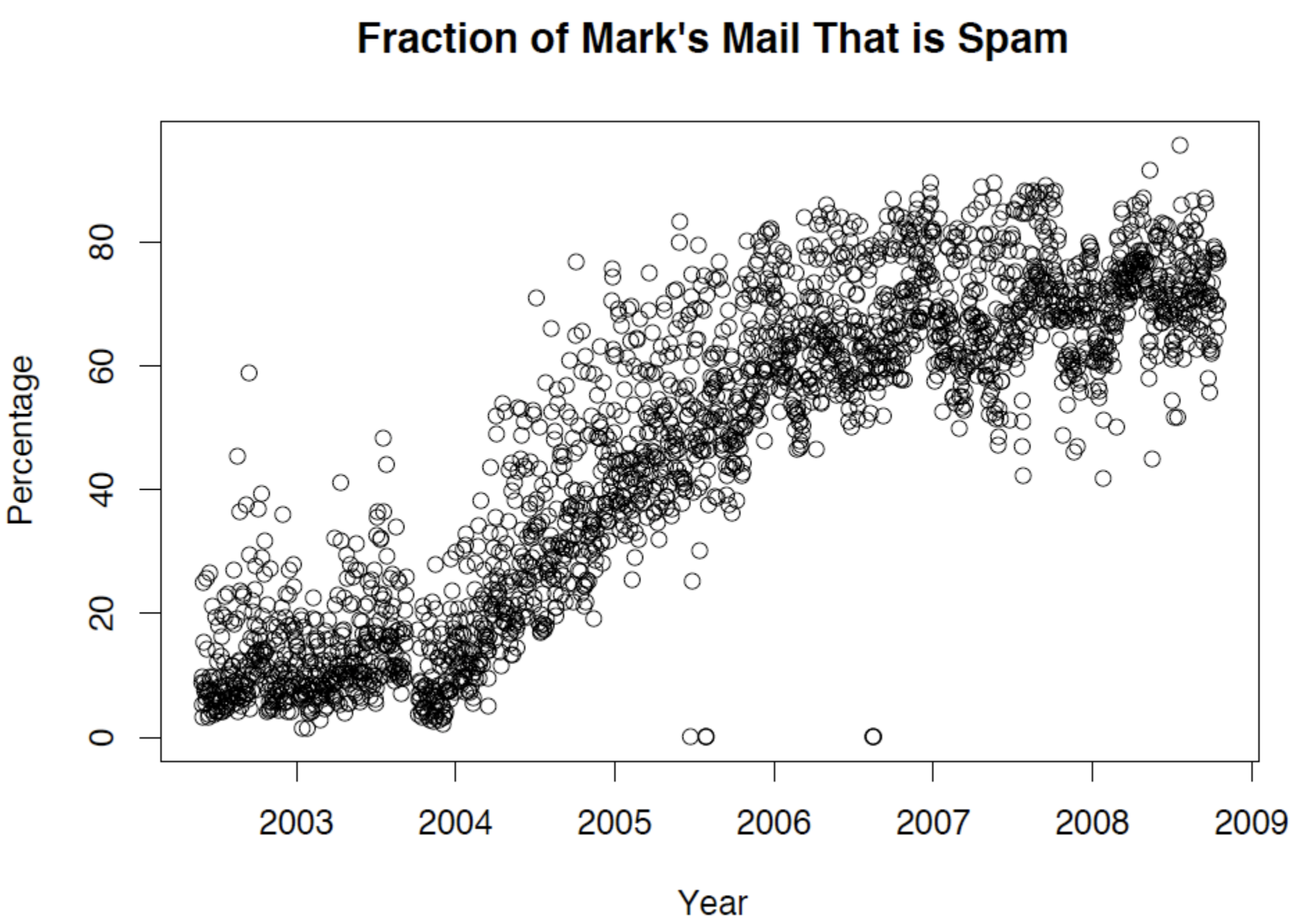


Know Your Enemy

- A sophisticated underground economy has emerged to profit from Internet subversion
- Empowered by virtually endless supply of "bots"
  - Internet systems under complete attacker control
- Dirt-cheap access to bots fuels *monetization* via relentless torrents of **spam**


Mark Allman's Non–Spam Mail
Messages Per Day
0
200
400
600
800
2003
2004
2005
2006
2007
2008
2009
Year


Mark Allman's Non–Spam + Spam Mail
Messages Per Day
0
200
400
600
800
2003
2004
2005
2006
2007
2008
2009
Year


Fraction of Mark's Mail That is Spam
Percentage
0
20
40
60
80
2003
2004
2005
2006
2007
2008
2009
Year

Know Your Enemy

- A sophisticated underground economy has emerged to profit from Internet subversion
- Empowered by virtually endless supply of "bots"
  - Internet systems under complete attacker control
- Dirt-cheap access to bots fuels *monetization* via relentless torrents of **spam**

- ***Just how profitable is all of this?***

Are Bots & Spam the New Black Gold?

Storm worm 'making millions a day'

Compromised machines sending out highly profitable spam, says IBM security strategist

Clive Akass, Personal Computer World 11 Feb 2008

The people behind the Storm worm are making millions of pounds a day by using it to generate revenue, according to IBM's principal web security strategist.

Joshua Corman, of **IBM Internet Security Systems**, said that in the past it had been assumed that web security attacks were essential ego driven.

- Spam finance elements:
  - Retail-cost-to-send vs. Profit-per-response
  - Key missing element: spams-needed-per-response, i.e., *conversion rate*

How can we **measure** this?

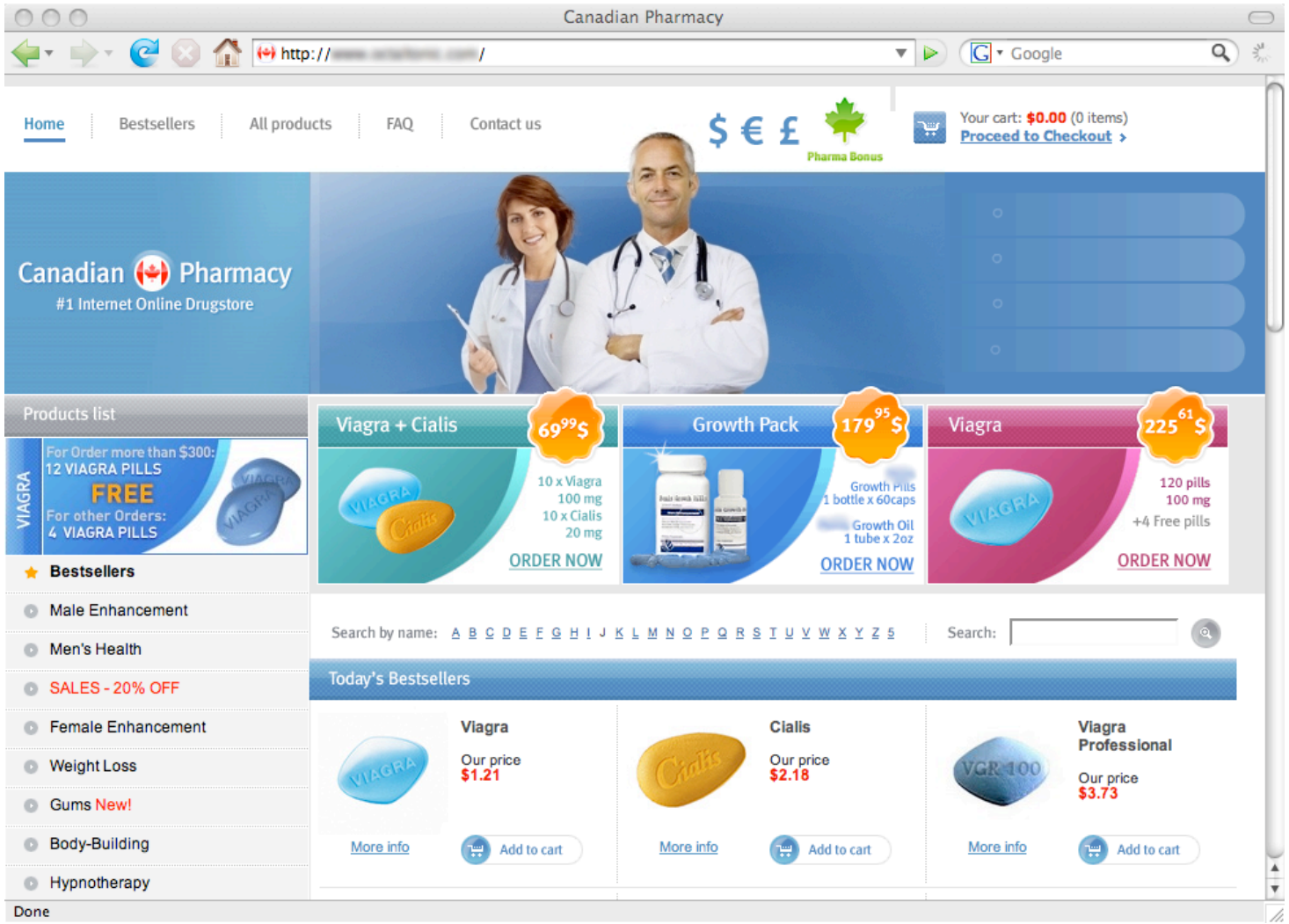
Welcome to **Storm**!

Would you like to be one of our newest bots?

Just read your postcard!

(Or even easier: just wait 5 seconds!)

Welcome to **Storm**! What can we sell you?

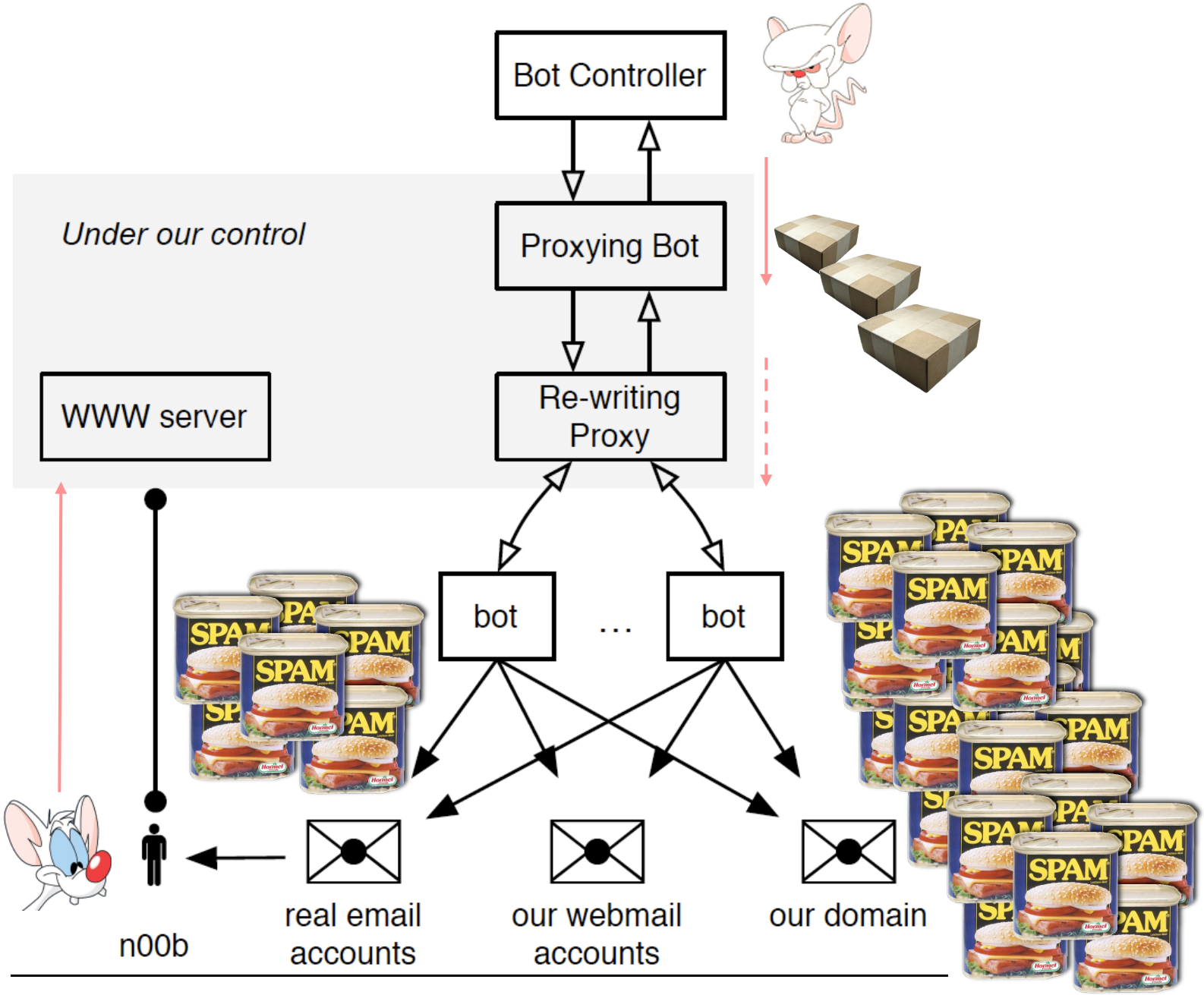


These folks seem trustworthy …

… how about these?

Botnet Infiltration

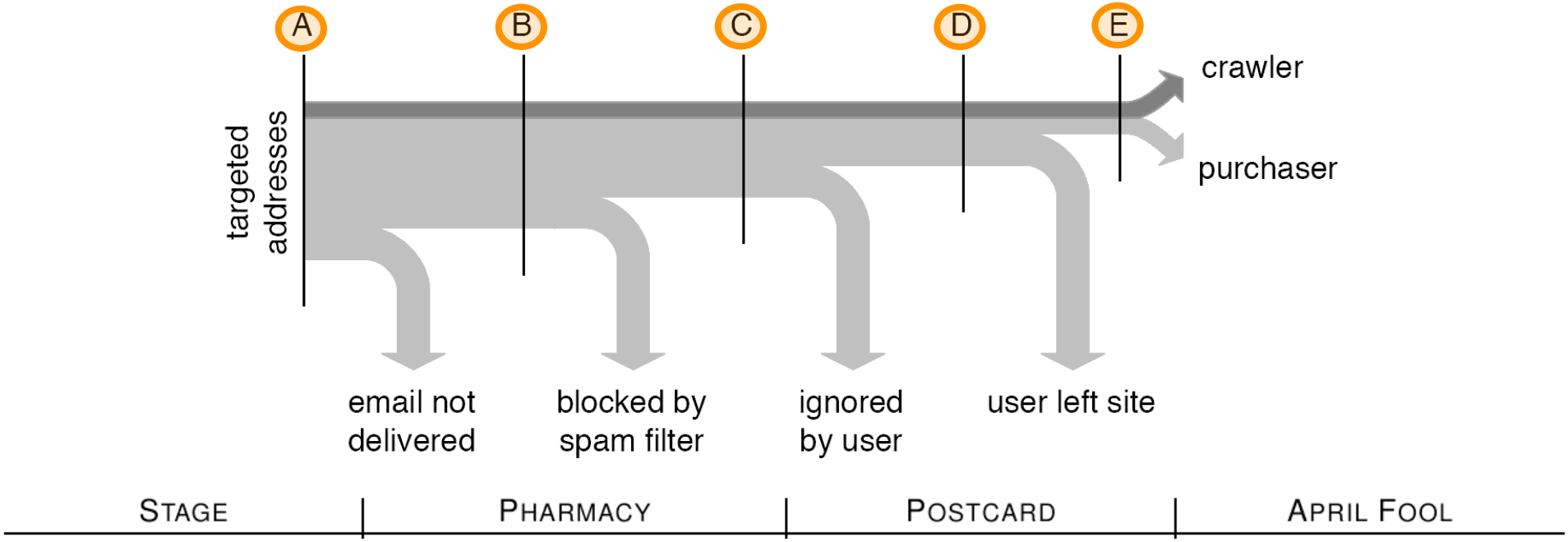
- Thanks to *E-Card* spam, we can easily acquire Storm bot binaries …
  - … and run them within the controlled GQ environment
- Storm instructs some of its bots to serve as Command-and-Control (*C&C*) proxies
  - Relay commands from botmaster to "workers", send back results
- With a lot of elbow grease, we reverse-engineered the C&C protocol …
- … so we can record all spam sent through us …
- … and in fact **rewrite** spam directives so that E-Card / Pharma URLs come to **our** (*defanged*) web sites


Bot Controller
Under our control
Proxying Bot
WWW server
Re-writing Proxy
bot
…
bot
real email accounts
our webmail accounts
our domain
n00b

Campaign volumes - Spring 2008

CAMPAIGN	DATES	WORKERS	E-MAILS
Pharmacy	Mar 21 – Apr 15	31,348	347,590,389
Postcard	Mar 9 – Mar 15	17,639	83,665,479
April Fool	Mar 31 – Apr 2	3,678	38,651,124
		Total	469,906,992

Conversion rates

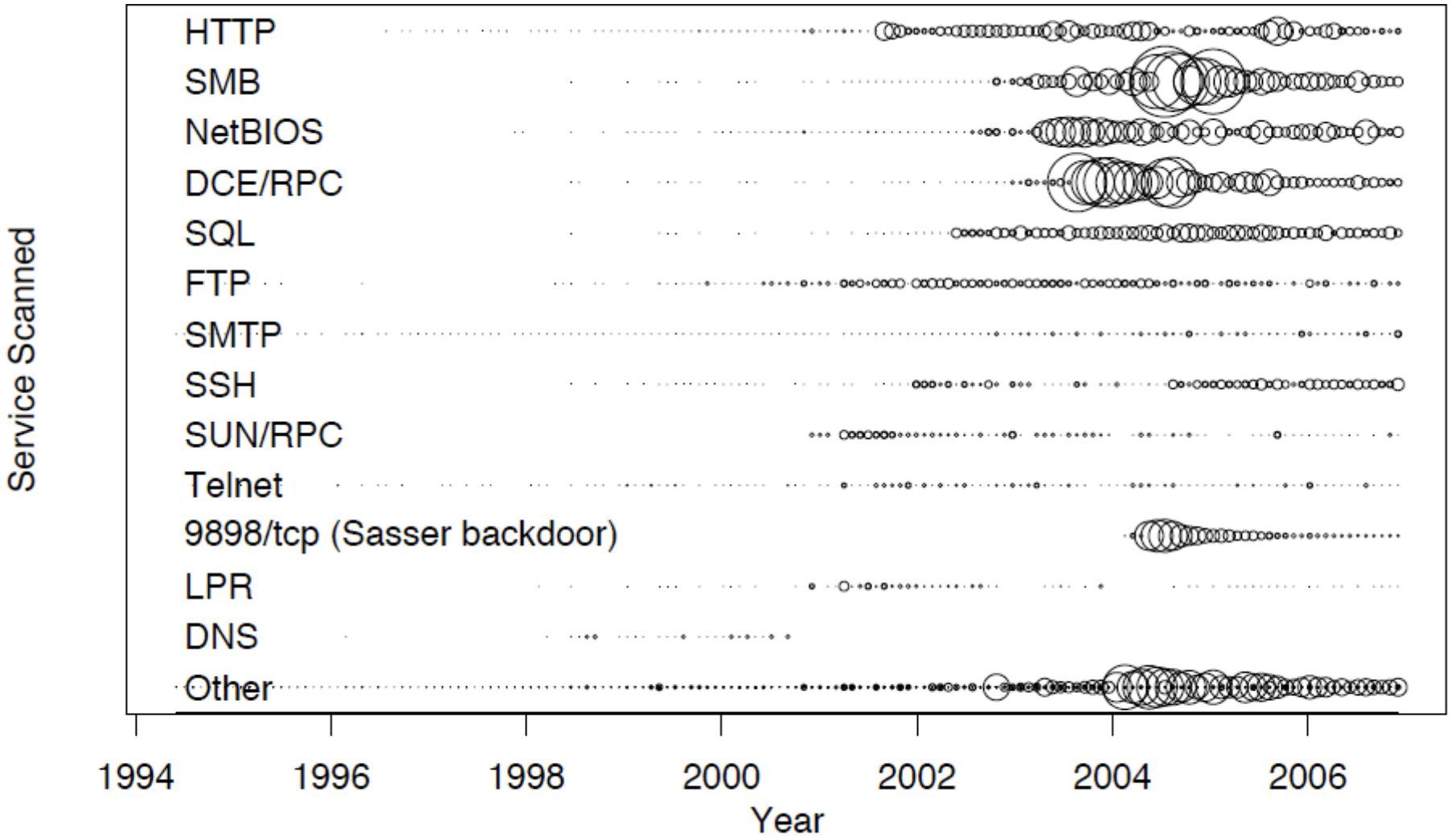


Storm Revenue

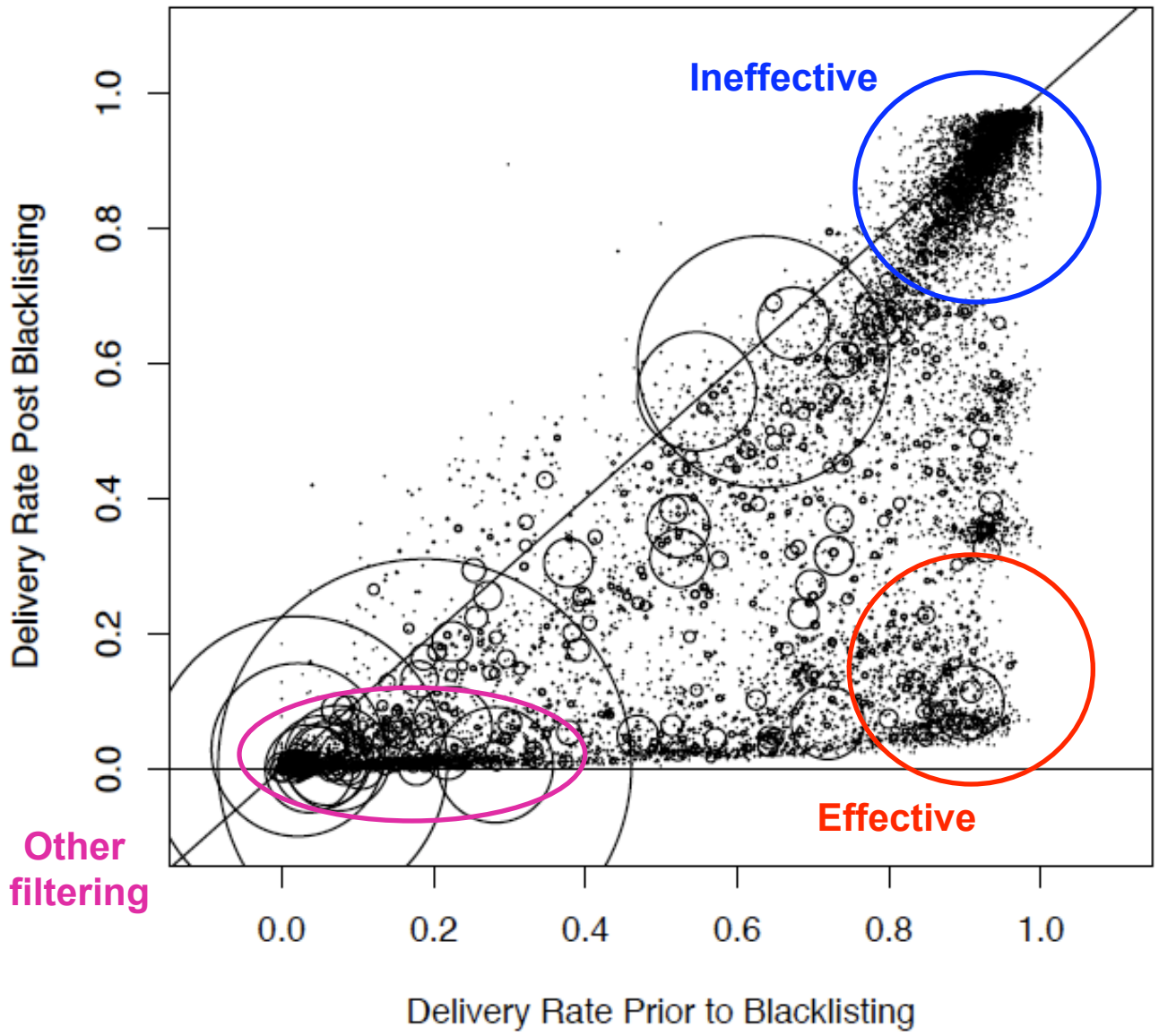
- 28 purchases in 26 days, average “sale” ~$100
  - Total: $2,731.88, $140/day
- **But**: we interposed on only ~1.5% of workers:
  - $9,500/day (8,500 new bots per day)
  - $3.5M/year
    - Though if selling Viagra via *Glavmed affiliation*, cut is **40%**
- Storm: service provider or integrated operation?
  - Retail price of spam ~$80 per million
    - Pharmacy spam would have cost 10x the profit!
  - Strongly suggests
    Stor
    m
    operates as an integrated operation rather than a reseller

Summary

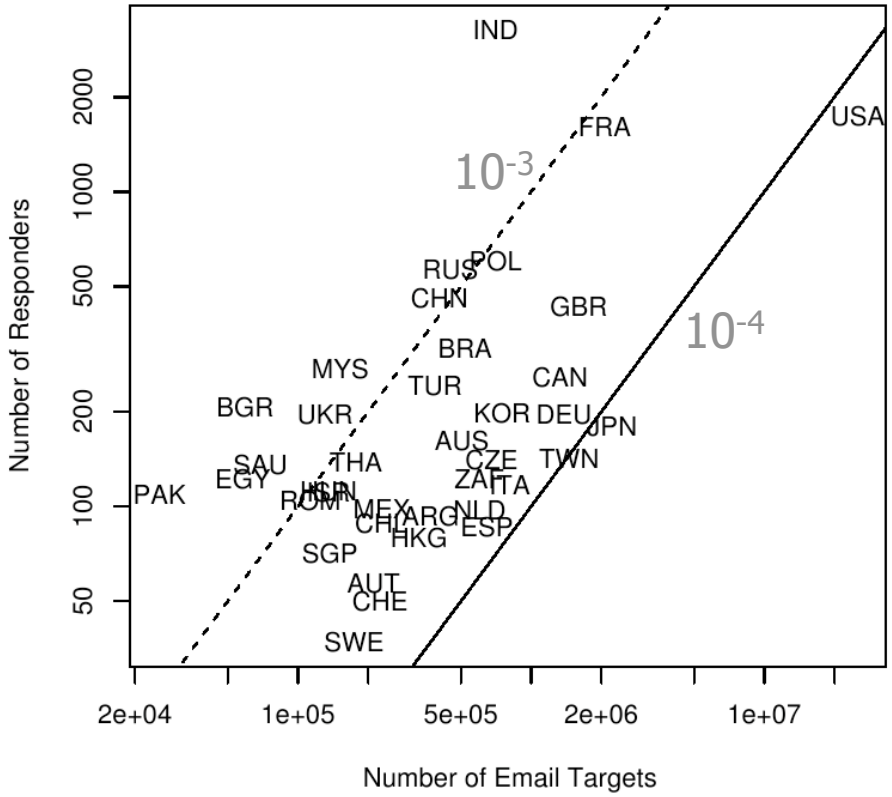
- Network security research has seen enormous change over ICSI's lifetime
- From:
  - Not a field …
  - … to fending off ardent amateurs
  - … to global worm epidemics
  - … to botnets employed for spam campaigns that fuel an emergent underground economy
- The first of these was pretty tenable (and fun!)
- The second was daunting but the field made some surprising advances
  - Though cyberwarfare remains a huge latent threat
- The third is even more daunting …
  - … deeply worrisome because it's fueled by criminals out to make money - **hastening the pace of adversary innovation**

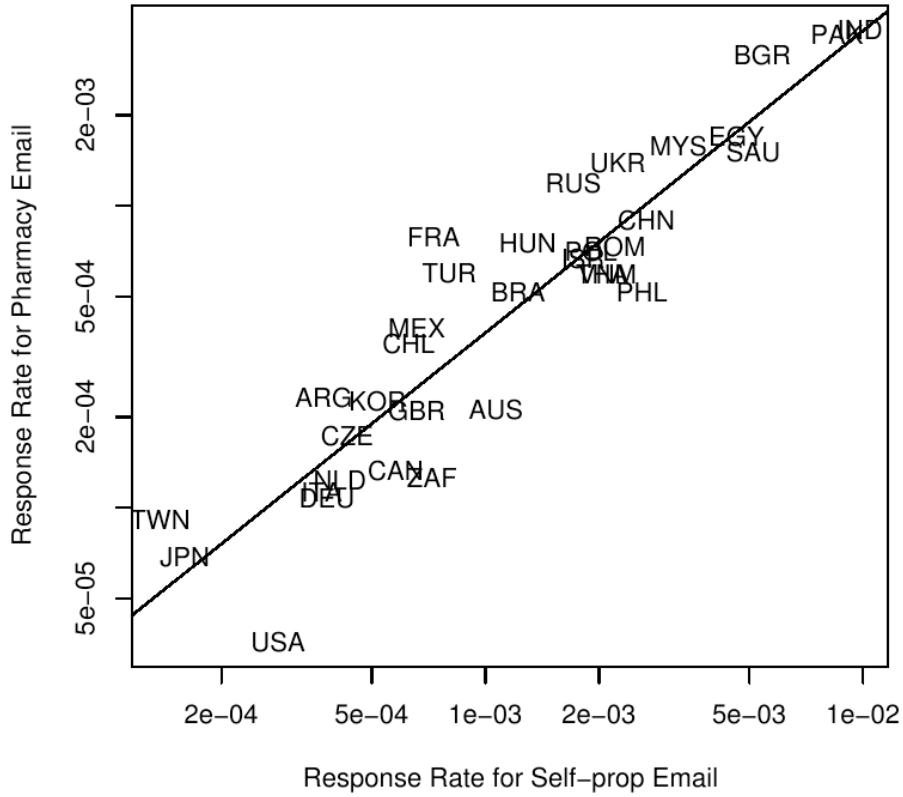

Service Scanned
HTTP
SMB
NetBIOS
DCE/RPC
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
1994
1996
1998
2000
2002
2004
2006
Year

Effects of Blacklisting on Delivery Rates



Conversion Rates For Different Countries





Time-to-click distribution