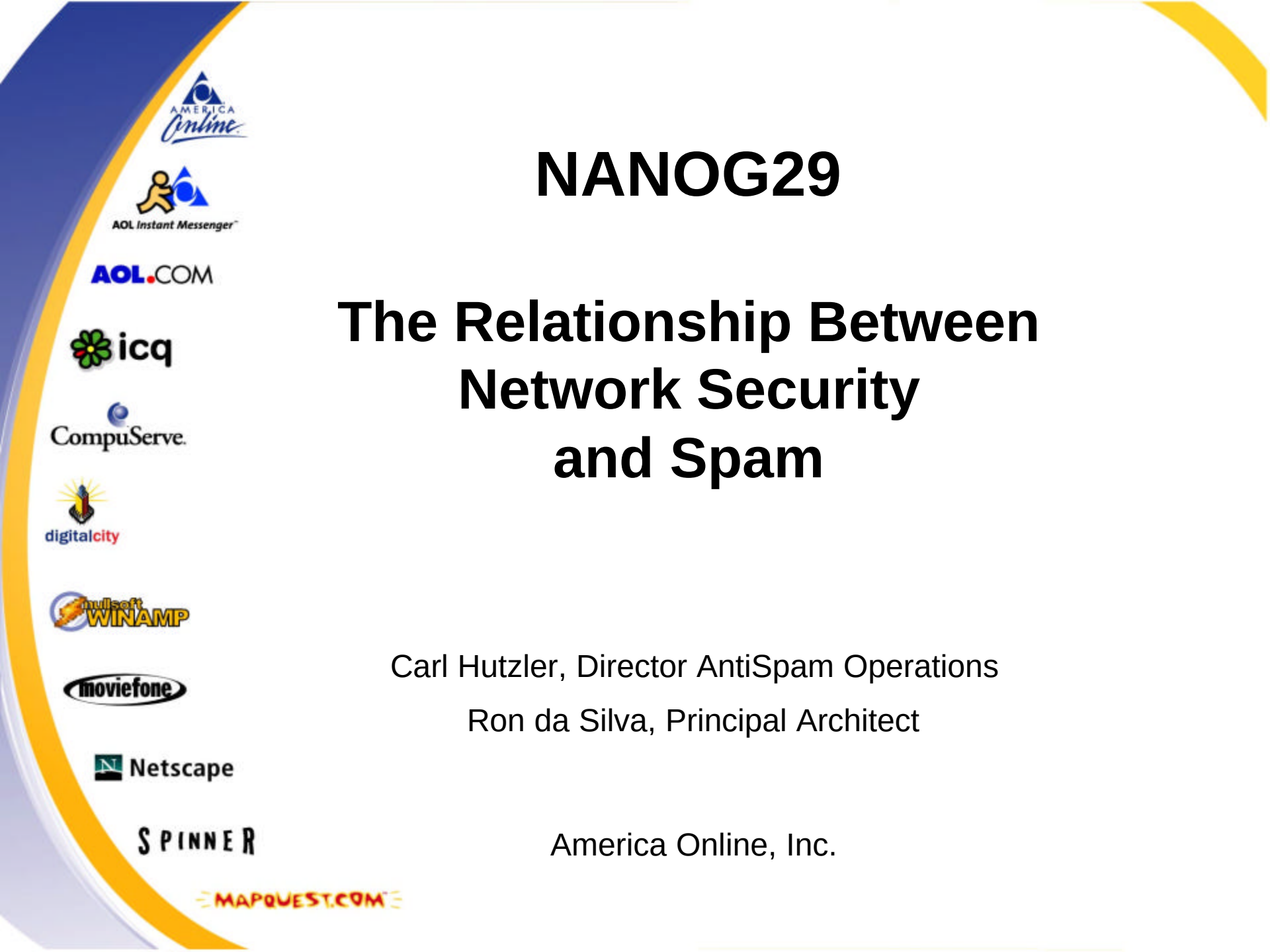


NANOG29

The Relationship Between Network Security and Spam

Carl Hutzler, Director AntiSpam Operations

Ron da Silva, Principal Architect

America Online, Inc.

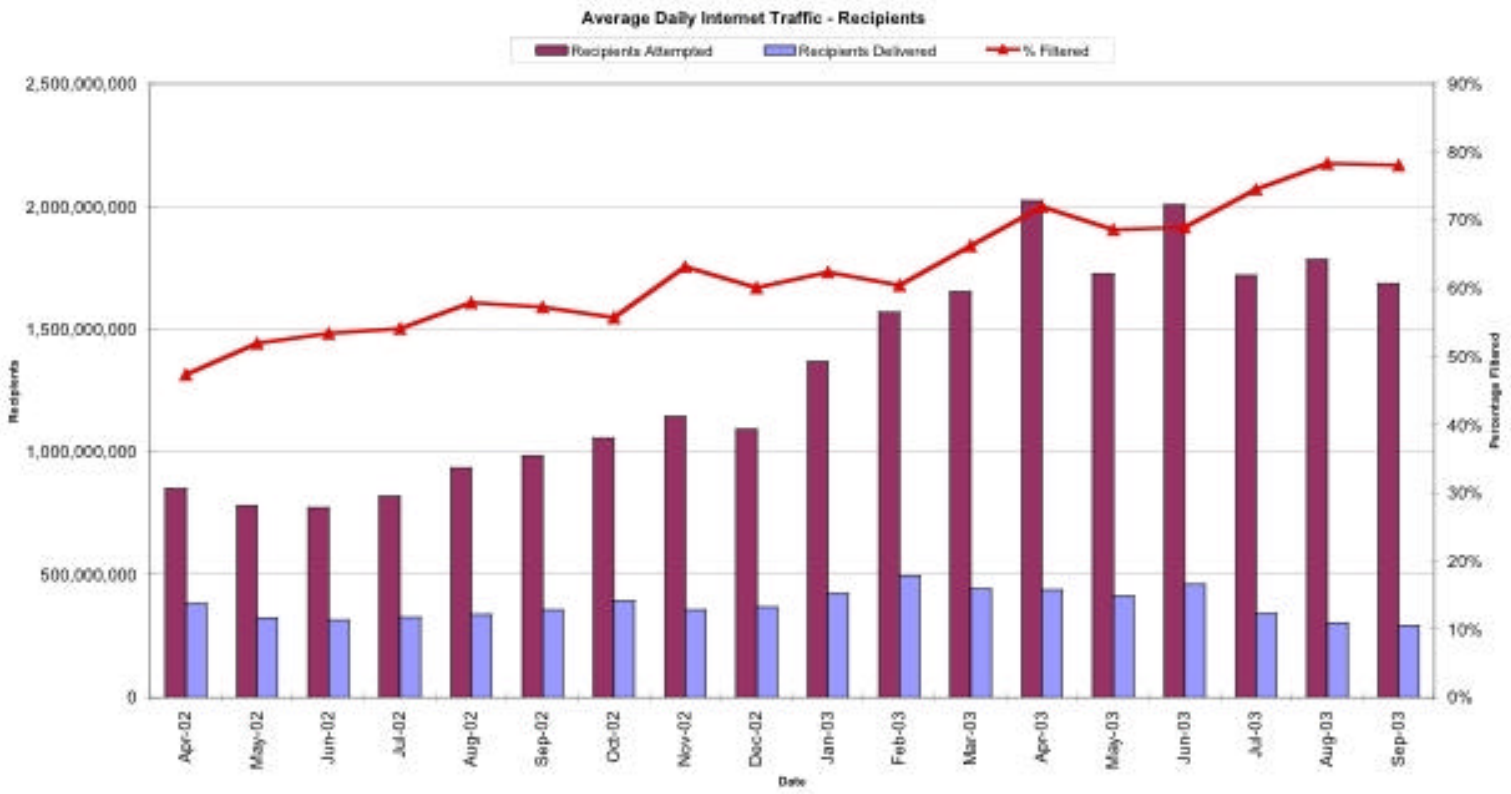
Executive Summary

- **Spam is a large and growing problem for AOL**
  - AOL now blocks over 80% of inbound Internet spam emails sent to AOL members (up to 2.4 billion per day)
  - The number of attempted spam emails to AOL has almost doubled every year for the last 6 years.

- **Spam is our #1 member complaint**
  - Significant number of members say spam is what they like least about AOL
  - Spam disproportionately affects our most valuable customers
  - Members report 4-6 million complaints daily

Attempted Mail vs Delivered to AOL.COM

(daily average over a given month)



The Spammer Formula

Total Spam = Messages x Recipients x IP Addresses x Accounts

- Spammers must be able to send millions of messages per day.
  - Typically 1M to 50M or more!
- Many solid controls are in place to prevent this behavior
  - Limits on how many messages per IP
  - Limits on how many message/IP/time
  - Limits on how many messages per account
  - Limits on how many complaints per IP
- Problems arise when the spammers have a very large or unlimited amount of any one or more variables in the formula

How To Combat SPAM?

- Block “known” bad senders
- Filter based on “rate” data
- Filter based on “envelope” data
- Filter based on “clickable URLs”
- Use member reports to tune filters
- Engage “legitimate” mailers in dialogue
- Take “bad apples” to court…

…but this is not enough!!

A majority of today's Spam can be traced to network and application security issues

- **IP Space Hijacking**
- **Malware infected PCs**

- Open Proxies and Relays
- Insecure Registration Systems
- Account Harvesting
- Insecure Applications like formmail, unpatched appliances

IP Space Hijacking

IP Space Hijacking

- How can we allow a hacker to steal IP space and route it to any location they like?
  - Social Engineering?
  - BGP Routing?
- How can we detect this behavior such that we can counter it quickly?
- How can we stop their capacity to do this in the first place?

```
OrgName:    Inform, Ltd.
OrgID:      INFORM-12
Address:    1123 2nd Ave
City:       San Francisco
StateProv:  CA
PostalCode: 94103-2705
Country:    US
NetRange:   143.49.0.0 - 143.49.255.255

CIDR:       143.49.0.0/16
NetName:    INFORUM
NetHandle:  NET-143-49-0-0-1
Parent:     NET-143-0-0-0-0
NetType:    Direct Assignment
NameServer: NS1.INFORMLTD.COM
NameServer: NS2.INFORMLTD.COM
Comment:
RegDate:    1990-03-26
Updated:    2003-02-20

TechHandle: ZI110-ARIN
TechName:   Inform Systems
TechPhone:  +1-555-555-5555

TechEmail:  ipadmin@informltd.com
```

Hijacked IP Space for Purchase

home | my eBay | site map | sign in/out

Browse | Sell | Services | Search | Help | Community

item view

See this item in eBay's new look for this page.

/16 CLASS B - 65534 IP's GRANDFATHERED !!!!

Item # 3029809556

Electronics & Computers:Networking & Telecom:Other

Electronics & Computers:Wholesale Lots:Networking & Telecom

Description

Bid!

Current bid	**US $6,800.00** (reserve not yet met)	Starting bid	**US $0.01**
Quantity	**1**	# of bids	**29** Bid history
Time left	**8 days, 0 hours +**	Location	**Houston**
		Country/Region	**United States /Houston**
Started	Jun-09-03 22:34:11 PDT	Mail this auction to a friend	
Ends	Jun-19-03 22:34:11 PDT	Watch this item	
		Featured Auction	

Seller (rating)

csutter2002 (170)

Feedback rating: **170** with 100% positive feedback reviews (Read all reviews)

Member since: Jun-23-02. Registered in United States

View seller's other items | Ask seller a question | Safe Trading Tips

IP Space Hijacking

- Litigation updates
  - VA/CA/etc. anti-SPAM laws
  - identity theft
    - intent to appear as previous owner of address block by incorporating under same name
    - asserting use of block by forged email to update/redirect contact data with RIR
- Public policy initiatives
  - federal SPAM legislation
  - clearly define address ownership issues
    - ip addresses are “leased”
    - public resource that cannot be owned

Compromised/Hacked PCs and Hosts

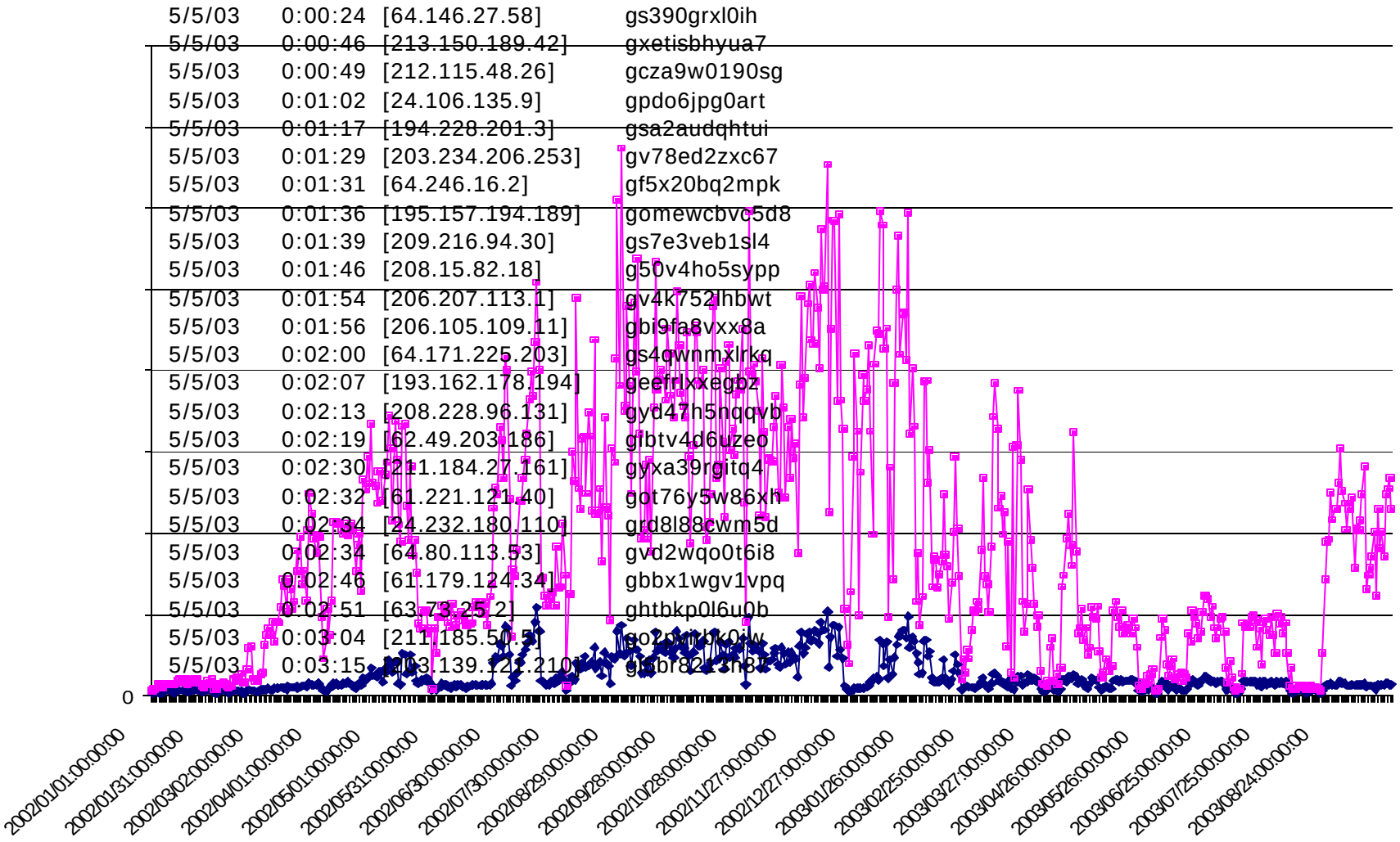
Malware Infected/Hacked PCs

- Millions of hosts are compromised on a good day. AOL has over 100 Million of these IPs blocked on our routers!
- Use of Malware (such as Trojans), Worms, and Virii
  - SoBig.[a-f]
  - ProxyGuzu
  - Lovegate
  - Jeem
  - IRC/Backdoor.g
  - AnalogX-Proxy.ldr
  - Illusion Mailer
- Exploiting vulnerabilities in operating systems and applications
  - Remote Control
  - Proxies and Relays

What do Spammers do with Infected Machines?

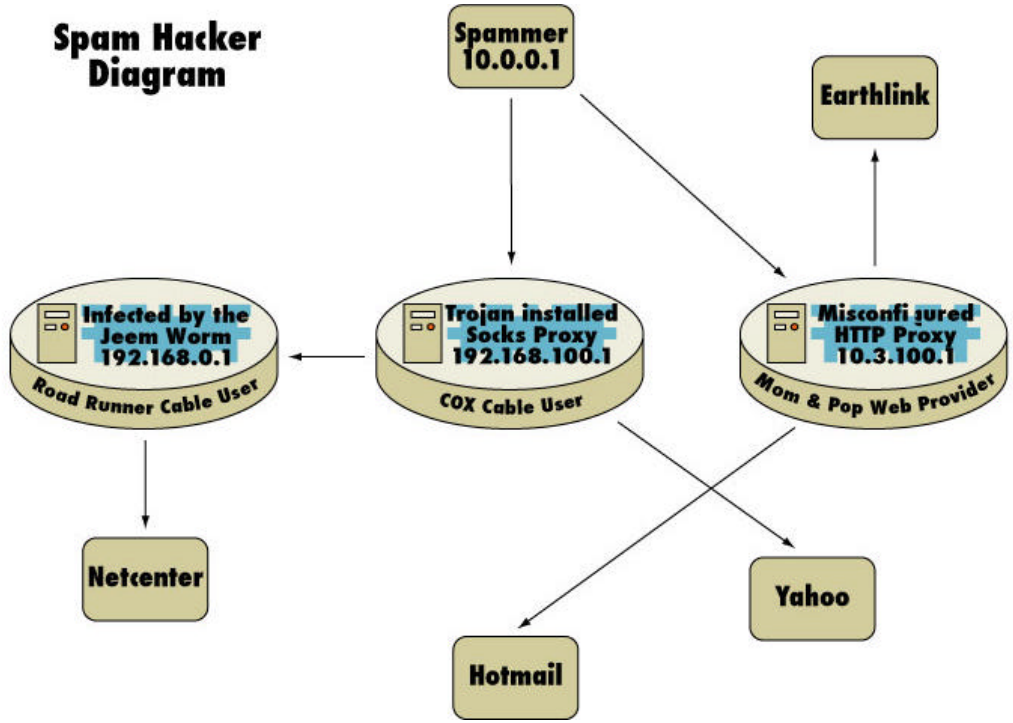
- Answer: Just about everything!
  - DDOS
  - Register Millions of Fraudulent Accounts at ISPs, EBAY, etc
  - Avoid Identity, traceability
  - Spam via millions of open relays
  - Host porn sites
  - Steal account passwords, credit cards

Register Millions of Free Email Accounts for Spamming



What to do about infected PCs?

- How can we detect them?
- How can we prevent their infection in the first place?
- Should we shut them down (disable access)?



Conclusions

- Large ISPs like AOL have deployed sophisticated blocking, rate limiting, and filtering technologies which are forcing spammers to find new methods.
- In order to blend in, spammers like finding IP space and/or accounts on major ISPs. We are forcing them to the ISPs
- Spammers are likely paying hackers to provide IP space for them to utilize with the goal being to spread out the volume across many IPs to blend in.
  - Many of the techniques hackers use are more and more criminal and disruptive in nature

Network and Application Security are more important than ever.

Ever Wonder How Spam Free Your Network Is?

- Call 703-265-4670 or 888-212-5537 and select the AOL Postmaster
- Request a Complaint Feedback Loop
  - Have your IP space available (CIDR or otherwise)
  - Have an email address where you would like the spam reports sent
- We will send the reports as we get them from our members in real-time
- Reports will have the full content and original headers intact.

- Any issues, contact: cdhutzler@aol.com