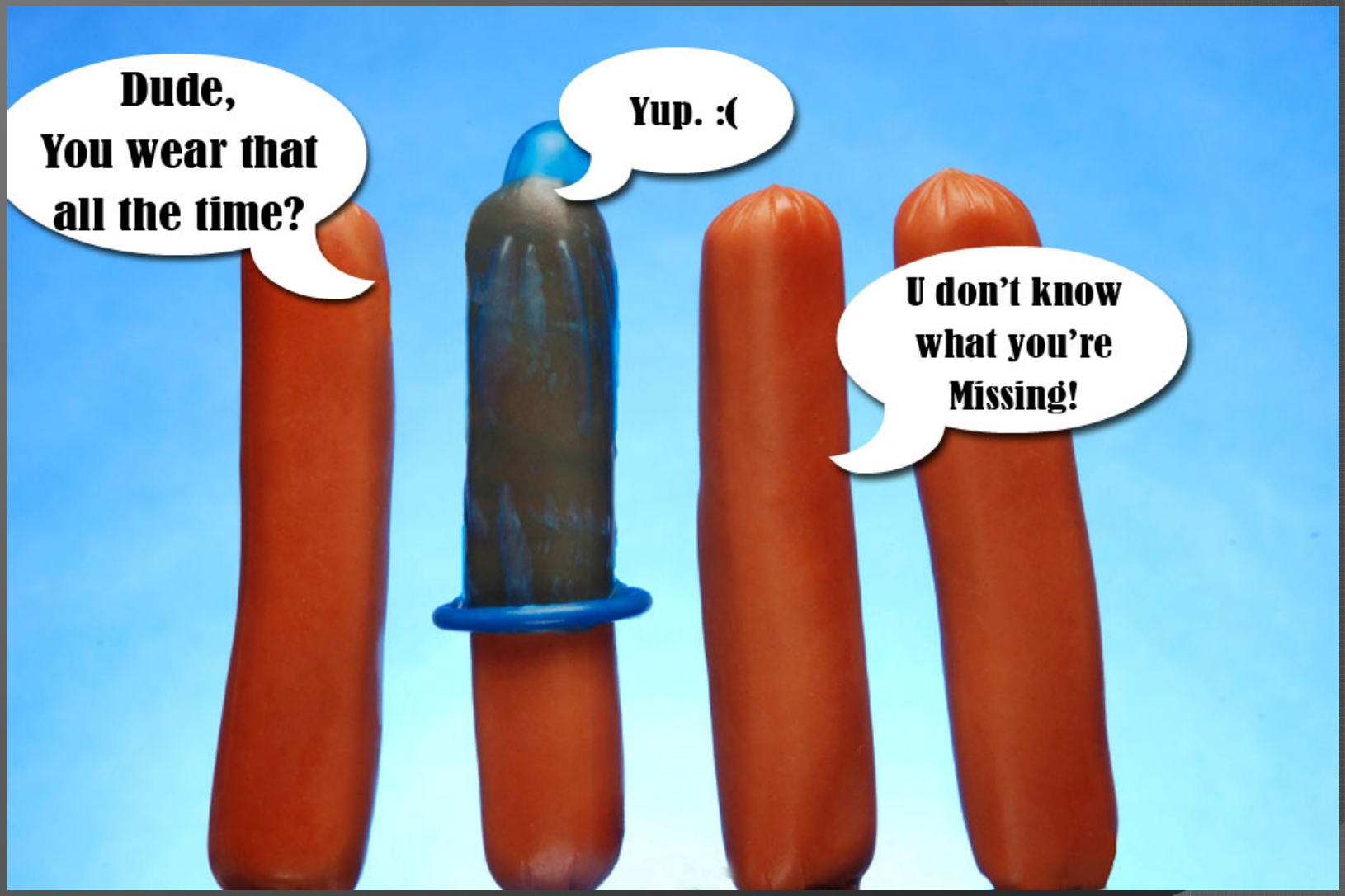
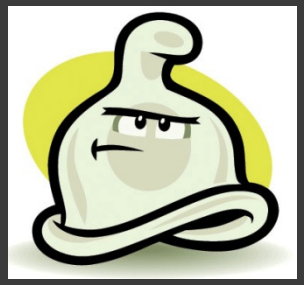


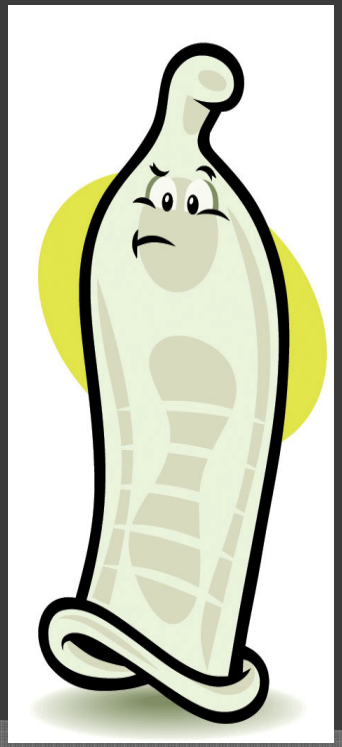
FORCED INTERNET CONDOM 2008

History

- We have spammers to thank for this
  - History of spam --- According to ME
    - First open mail relays
    - Throw away dialup accounts using the ISP relay
      - Playing ISPs against each other to prolong the account
      - Spammers eventually started not using ISP relay
    - Led to SMTP outbound port 25 filters

History continued…





- The players?
  - Nanog, news.admin.net-abuse.email, VIXIE RBL, ORBS
- Ultimate Driver - Money
  - The *real* Players, UUnet, PSI, Sprint Dial
    - Their customers (Earthlink, Mindspring, AOL, etc…) needed the solution the most
  - Was there opposition to 25 filters? Absolutely.
    - Privacy advocates didn't want to force users into a "Check point"

History Continued

- Filtering was a technical problem
  - ACLs were scary – how can we manage this?
    - Line speed filtering without CPU impact?
- The technical challenges were solved
  - A new “tool” was created
  - A process in place
  - But we won’t do anything else with this

So now we have this new tool

- What's next?
  - Spam isn't the only thing "bad" on the Internet
  - SunRPC TCP 111 --- Solaris exploits
    - Code Red ~2001 – port 80
  - NetBios, Windows95 winuke
    - Windows 98, --- NT4.0, 2000
      - Oh you can do more with Netbios? Neat
      - WindowsXP ---
  - SQL Slammer ~2003
    - 1433tcp – 1434udp

What is being filtered?

- TCP
  - 21, 25, 80, 111, 135-139, 445, 1434, 1433, 3128, 4662, 37681…….
- UDP
  - 161, 1434, 135-139, 445
    - What about other protocols?

What is being filtered continued…

- First pass – a manual process
- How we collected the first round of data
  - Send packets outbound
    - nmap -sS -P0 -T 4 -p0-65535 yy.yy.yy.yy
  - Recipient
    - Tcpdump –i eth0 -r capture_inbound.pcap host xx.xx.xx.xx
  - Process in reverse

Filters continued...

- Need a larger sample of data
  - UDP – Forget it
  - Running full portscans wasn't possible
    - Limited to the subset of ports from the manual tests
      - 25,139,445,6343,4662,6699,21,136,137,138,9729,25970,111,34427,37681,48889,49807,61771
  - Requirements
    - Needed a tool everybody can run
    - Web based? Sure why not

PORTSCAN.us

- Test outbound ports --- Easy
  - The Process
    - URL strings and image tags:
      - http://portscan.us:25/phpLibs/get_image.php
      - http://portscan.us:139/phpLibs/get_image.php
      - http://portscan.us:445/phpLibs/get_image.php
- Just for fun: http://port139online:139/

Portscan.us continued

3. Right-click in the "Preferences" area, choose New->String
4. For name enter 'network.security.ports.banned.override' and hit "Ok"
5. For value enter '25,139,445,6343,4662,6699,21,136,137,138,9729,25970,111,34427,37681,48889,49807,61771' and hit "Ok"
6. Refersh this page and continue to fill it out.

Your IP	68.225.89.199
Your Host	njektd.com
IP	68.225.89.199
ISP	AOL / Other...
Class of Service	Residential
Country	United States
State	Alabama
Zip Code	
Comments	Please put in any general comments about your ISP...

Submit

Portscan.us outbound tests

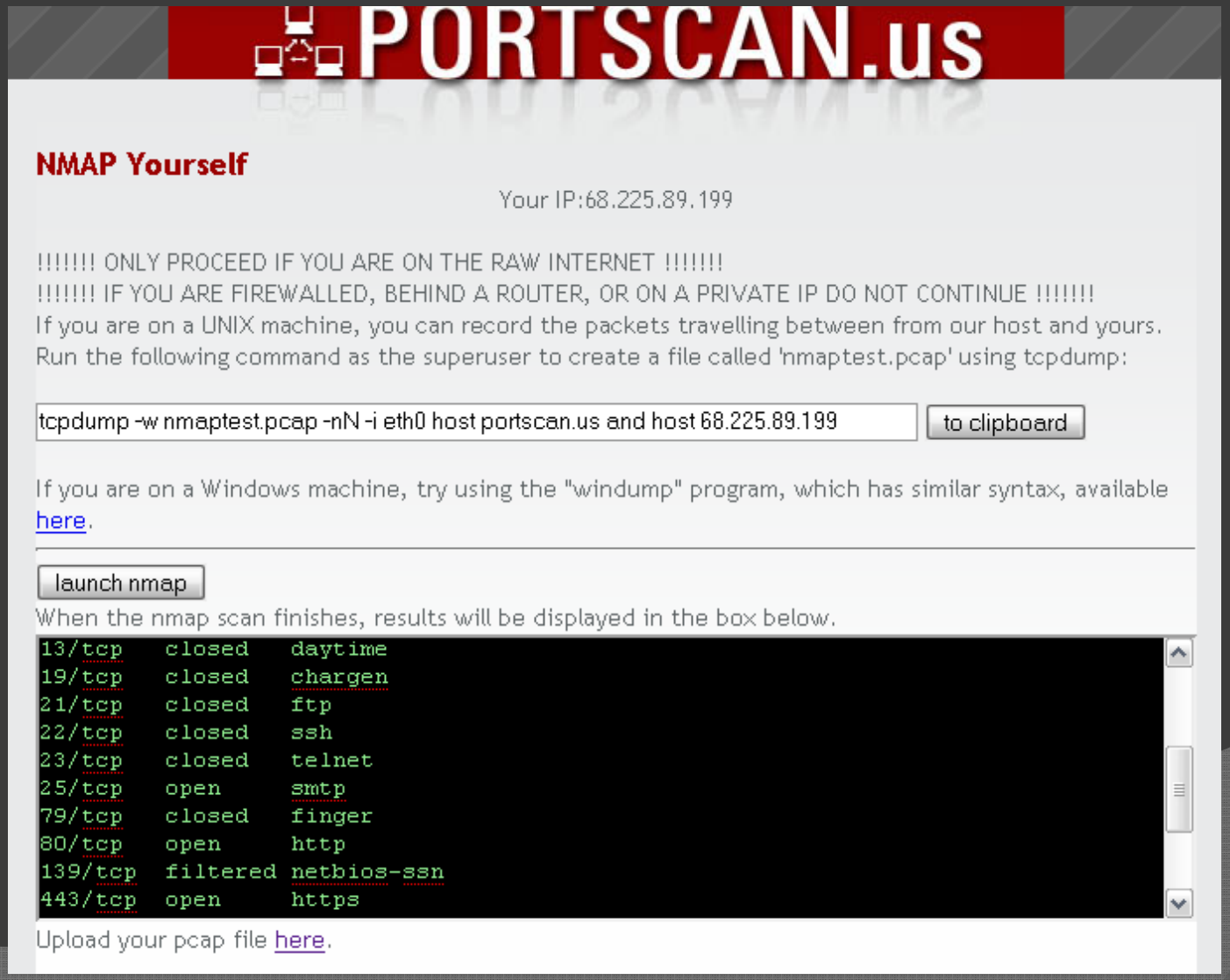
PORTSCAN.us

Thanks

Thank you for participating. Please DO NOT close your browser. You will be redirected when the test completes.

Connected: 80
Connected: 443
Trying Port 139...
Trying Port 445...
Connected: 6346
Connected: 4662
Connected: 6699
Connected: 21
Trying Port 136...
Trying Port 137...
Trying Port 138...
Connected: 9729
Connected: 25970
Connected: 111
Connected: 34427
Connected: 37681
Trying Port 48889...
Trying Port 49807...
Connected: 61771

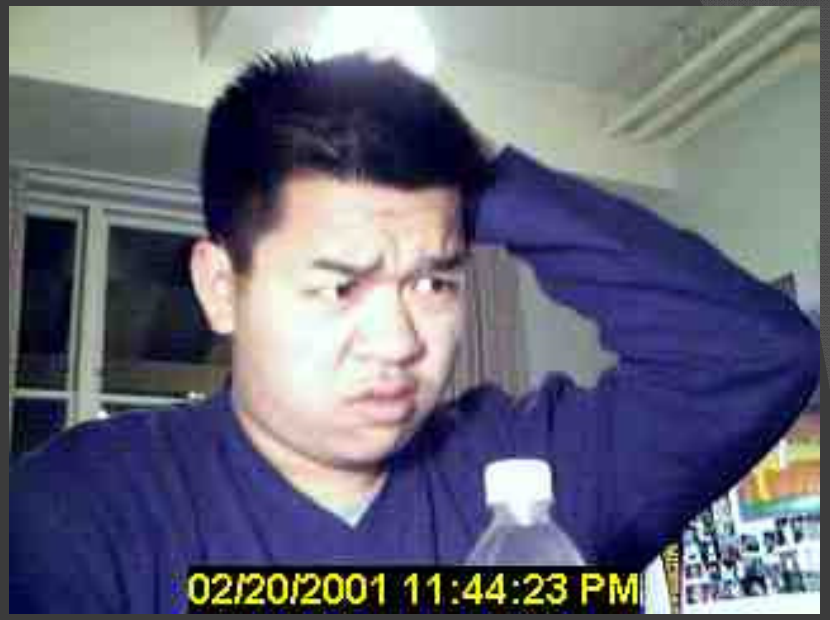
Portscan.us – nmap page



Portscan.us - inbound

- This proved be more difficult
  - We have much more outbound data
  - Users opted out
    - Users not savvy or NAT'd
    - Even with warnings many of our sample captures had private IP addresses in them

Results



- Ugh!
  - Inconclusive
  - Consistent
    - NetBIOS
  - Surprising to us
    - Port 21
  - Filtered ports changed
    - The same ports from 3 months ago
  - Can’t generalize “Comcast” or “RR” or “Cox”
    - Regionally operated
  - Follow the project at portscan.us

What is Internet service?

- How can an ISP change the rules or redefine Internet service whenever they want?
  - by *using* the service you agree to the Internet access agreement
  - “How will I know when Comcast changes this Policy?
  - **Comcast may revise this Policy from time to time by posting a new version on the Web site at http://www.comcast.net** or any successor URL(s) (the "Comcast.net Web site"). Comcast will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending e-mail announcements or posting information on the Comcast.net Web site. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Comcast High-Speed Internet Service should read any Comcast announcements they receive and regularly visit the Comcast.net Web site and review this Policy to ensure that their activities conform to the most recent version. You can send questions regarding this Policy to, and report violations of it at, http://www.comcast.net/help/contact/”

What is an Internet Service Provider?

- Do they only get you on the net?
- Does their service need to include protection?
- Do you expect your ISP to block spam?
- We're somewhat used to this changing on us?
  - Where did Usenet go?

Changing Internet, port filters, etc..

- People aren't that upset about this
  - There are a few privacy advocates
  - There are a few Internet purists that are upset
  - There are a few spammers that are upset
  - There are few security testers
- What did this really accomplish?
  - With respect to port 25, how could this have played out differently?
    - Would we have Gmail?
    - Or would the SMTP protocol have been fixed?

The Internet *is* changing

- And it's changing faster then the oversubscription model for selling bandwidth to consumers.
  - Internet was a more two way conversation
  - With widespread dial-up, it shifted to a one way medium and the technology
    - Users still don't want all their multimedia content in its current packaging

Tipping Point – Filters were Ok, but then….

- Something changed
  - ~October 2007 the first report of forged reset packets to throttle torrent seeders
    - We really don't know when it first happened
    - Smaller players could have been doing it longer
  - A lot of attention and a lot of focus.
  - More about this later….

Sandvine - Simplicta

- Sandvine: Read their paper
  - “Network Neutrality: A Broadband Wild West?”
  - http://www.sandvine.com/general/getfile.asp?FILEID=37
  - Seriously – Read this^

Simplicta

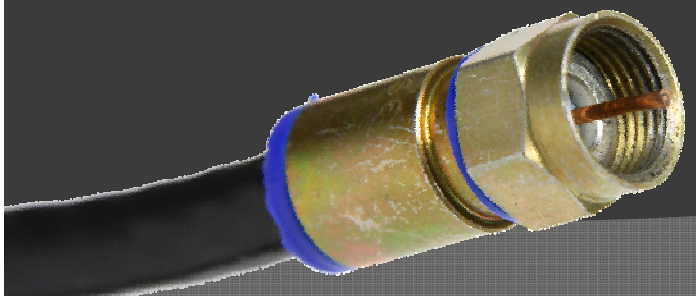
- What did Simplicta do before they were acquired by Sandvine?
  - Two products
    - Log aggregation and heuristic analysis of disparate data
      - Why? To identify *threats*
        - BOTS? Sure. P2P a threat? Depends on who you ask.
      - What else could you do with that?
        - Spy on competitors?
        - Maybe sell usage patterns? Think arbitron rating
  - "Controlling Internet Services with a DNS Traffic Switch: A New Technique to Fight Phishing Attacks and Clean Zombie Computers."
    - How would this product work if users didn't use the ISP DNS server?

Sandvine Continued

- So who is using it?
  - Check out the list of proud customers on sandvine.com --- oh you don't see any?
  - If this thing is restoring fairness to the Internet why don't ISPs advertise using it?

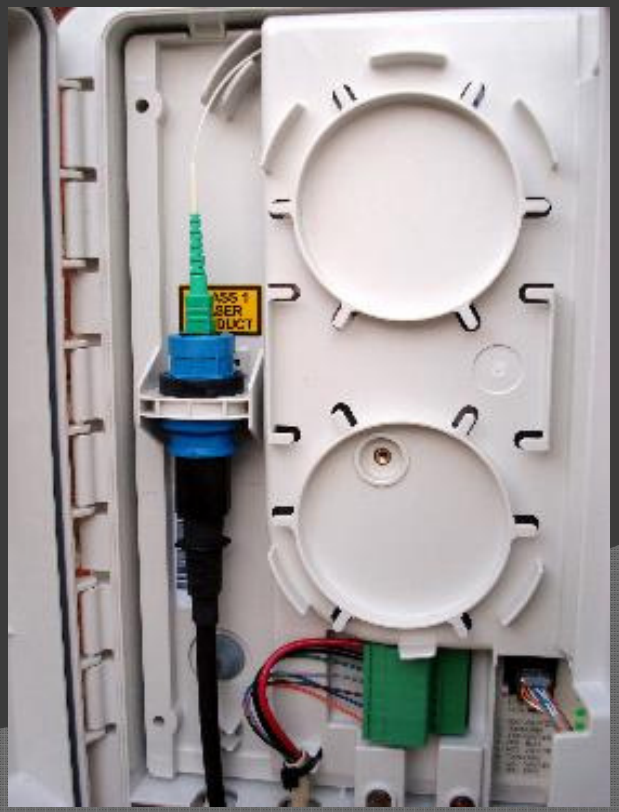
Sandvine Continued

- Let's imagine for a minute… who is the ideal customer?
  - Business model built on oversubscription of the one-way Internet
  - Couldn't plan for how the Internet is changing
  - ISP who is not Tier 1, who pays big bucks for strategic peering and bandwidth



Sandvine Continued

- Who probably *isn't* their customer?
  - "***Verizon rolls out "super-fast" 20/20 FiOS internet service***"




My LOST .. errr..UBUNTU Torrent isn't working!
Free Pr0n!
Lol CatZ!
How come I can't find Sex and the City?

Back to the resets...

- Investigations and reports
  - http://www.nnsquad.org/
    - “Hey my streaming interrupted”
    - “My SSH/telnet sessions keep dropping”
    - “My IRC connection keeps dropping”

Typical Network Behavior

- Other reasons for these reports
  - General packet loss from already saturated networks
  - DNS timeouts
  - Short DHCP lease
  - Slow computer
- People don’t have the tools or expertise to prove anything

Actual verified reports

- ~October 2007 – first capture packets showed the unsolicited Reset packets to Torrent seeders.
- Want to see Resets in action?
  - http://www.eff.org/wp/detecting-packet-injection

Why aren't there thousands of reports?

- Joe Ferren, a spokesman for the Cellular Telecommunications and Internet Association (CTIA) says:
  - *"*According to Ferren, no evidence of any widespread implementation of preferential network management is evident. "If it became common practice the other side of the debate would have a credible argument," he said."*
- Is this a real problem?
- The truth is it's not always on
  - The policy is defined by the ISP
  - Typical policy for Torrent might look something like this:
    - Number of active Seeds = 50 per node
      - If exceed number exceeds 50; send TCP resets

*Quote from: **Industry Groups Declare War on Net Neutrality**
http://www.internetnews.com/government/article.php/3728271

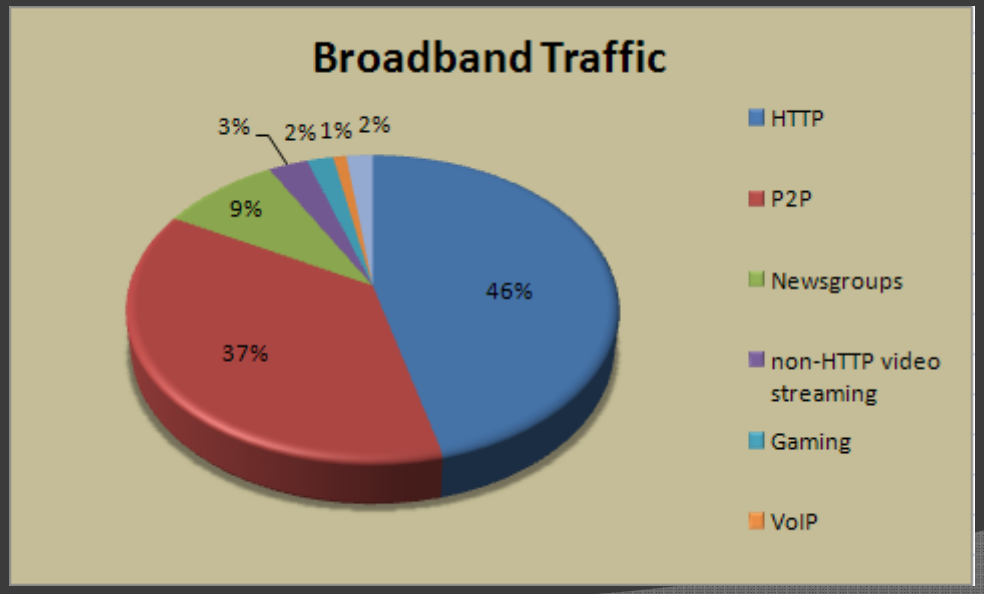
Why does *This* issue get so much attention?

- Because it's Change
  - Remember when VeriSign resolved all ".com" queries?

- A line was crossed
- It's a trust issue
- Fear of what's next to come
  - Favored Internet traffic, etc…

What now?

- Will this even matter?
  - What happened to email?
- The percentage of users who actually care about this is tiny.



Source:
http://arstechnica.com/news.ars/post/20070619-the-youtube-effect-http-traffic-now-eclipses-p2p.html

Their source:
Ellacoya Networks
(Network Management)

Apathy from fellow techies...

- “Shouldn’t these companies be able to operate their network anyway they want? After all, the user agreed to the terms of service?”
- “Just change your ISP”
- “But dude, they are doing it for the *Good* of the Internetz!”

What is Happening Now?

- FCC is pressuring ISPs for more open "Network Management" practices
- Petitions, complaints, and law suits filed
- "The Internet Freedom Preservation Act of 2008" - H.R. 5353
  - Introduced >this< week by Ed Markey (D-MA) and Chip Pickering (R-MS)

Where can this go?

- More lawsuits
- Is it really a good idea to have the Federal Government involved?
- Maybe the applications Evolve?
  - Giganews.com – Usenet over SSL
- Different Internet pricing model
- The cat and mouse game will begin.. Harder P2P clients, use of encryption, etc…
- Eventually a user will be sued or go to jail for
  - “Circumventing filter technology and causing service disruption”
    - Some how equated to “Cracking”
    - Then TOS will have to explicitly ban P2P

Wrap it up

- We've let things slide in the past
- We need to ask ourselves not
  - "What does this tool do?"
  - And instead "What else can this be used for?
- Full disclosure of "Network Management" practices
- Better notification practices for changes to the service or agreement

Thanks – Q&A

- Sites worth visiting
- http://www.freepress.net
- http://www.savetheinternet.com/
- http://www.nnsquad.org/