Trashing the Internet Commons: Implications for ISPs

Geoff Huston

May 2004

Thanks…

- Acknowledgement is given to Bernard Aboba and the Internet Architecture Board, where some of this material was originally collated as part of the IAB Plenary session at IETG59 in November
- The conclusions drawn from this material and the opinions presented here are those of the author

The Commons

- The Commons was an area of communal interest – people could use the common asset according to their needs on a non-exclusive basis
  - The necessary condition is that each person's use of the commons is 'considerate':
    - Fair and reasonable
    - Sustainable
    - Non-damaging
- The Commons represented the most efficient manner to apportion use of the common resource between competing diverse requirements
  - As long as everyone shares a consistent enlightened self-interest regarding fair use of the commons

The Internet as a Commons

- The Internet is an end-to-end mediated network.
- The Internet ‘middle’ does NOT:
  - Mediate between competing resource demands
  - Detect attempts to overuse the resource
  - Police ‘fair use’
  - Police attempts to abuse
  - Understand any aspect of end application behaviour
- *The Internet operates most efficiently when it can operate as a neutral commons*

Abusing the Commons

- The Commons is stable as long as all users share similar long term motivation in sustaining the Commons
  - It works for as long as everyone wants it to work
- The Commons is under threat when diverse motivations compete for access to the commons
  - Without effective policing, there are disproportionate rewards for short term over-use of the commons
  - Without effective policing, abuse patterns can proliferate
- Abuse of the Commons drastically reduces its efficiency as a common public utility

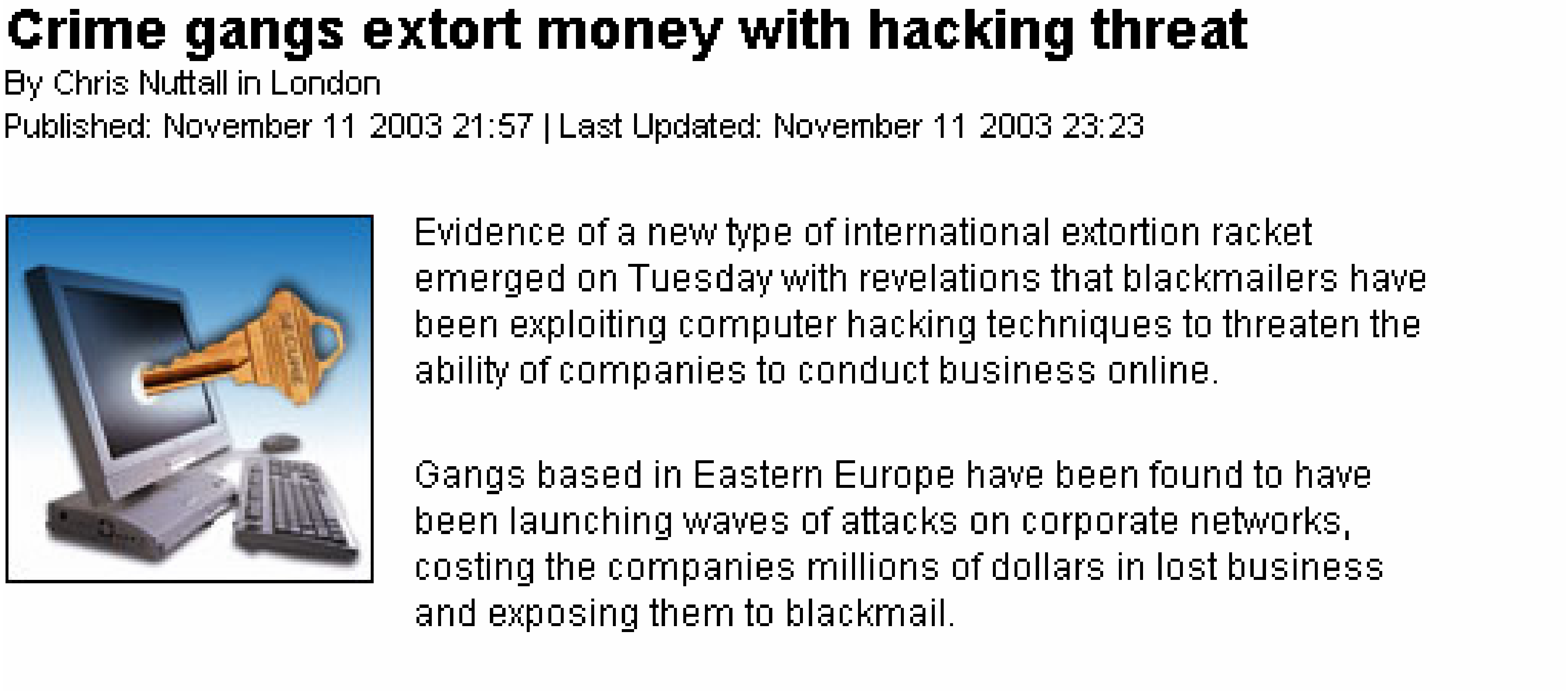
What’s the current state of the Internet Commons?

- Its being comprehensively trashed!

A Recent Headline

(London Financial Times, 11/11/2003)

http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1066565805264&p=1012571727088



Crime gangs extort money with hacking threat

By Chris Nuttall in London

Published: November 11 2003 21:57 | Last Updated: November 11 2003 23:23

Evidence of a new type of international extortion racket emerged on Tuesday with revelations that blackmailers have been exploiting computer hacking techniques to threaten the ability of companies to conduct business online.

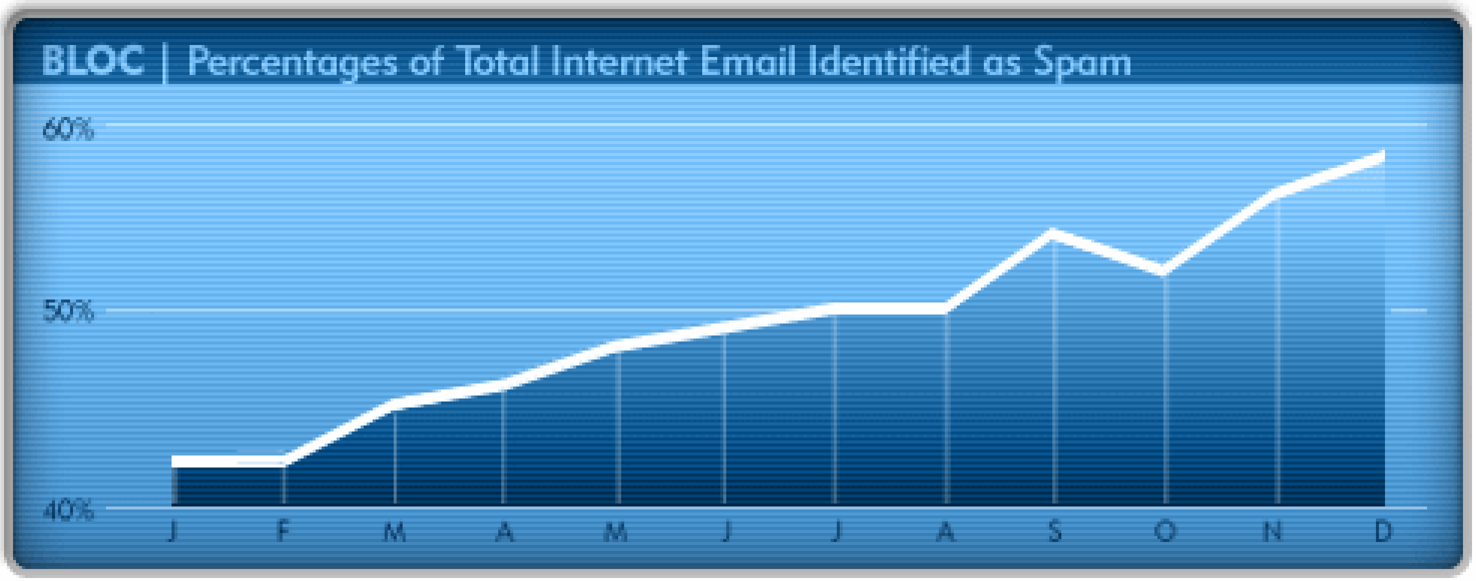
Gangs based in Eastern Europe have been found to have been launching waves of attacks on corporate networks, costing the companies millions of dollars in lost business and exposing them to blackmail.

Some Observations

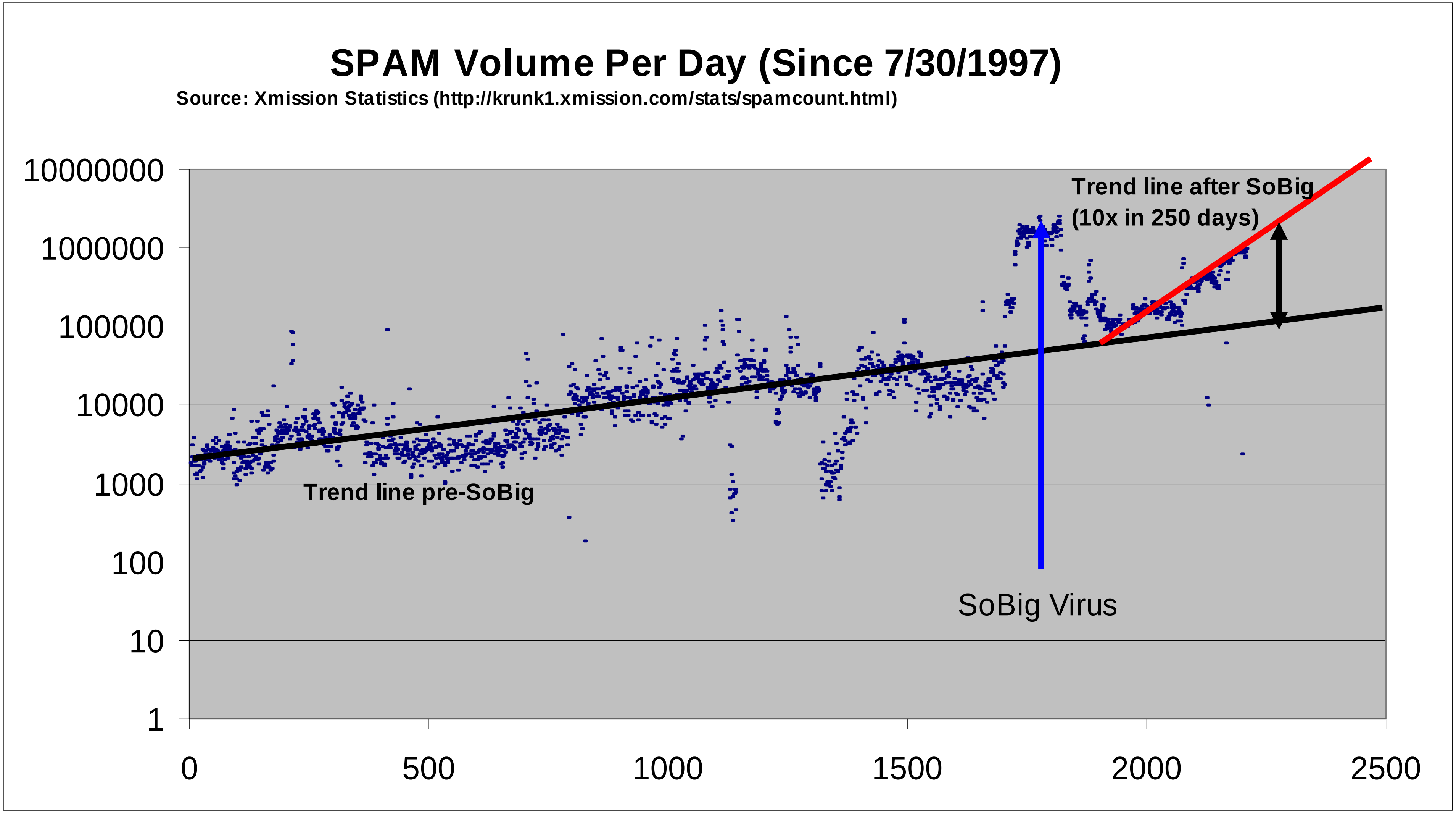
- The Internet now hosts a continual background of probe and infection attempts.
  - It has been reported that an advertised /8 sink prefix attracted some 1.2Mbps of probe traffic in mid-2003
- Its untraceable. Many of these probes and attacks originate from captured ‘zombie’ agents (distributed denial of service attack models)
- Many attack vectors use already published vulnerabilities
  - Some attacks are launched only hours after the vulnerability
  - Some attacks are launched more than a decade later
- Attacks are mounted both directly (e.g. port probes) and indirectly (e.g. mail-based virii)

Percent of Total Email Identified as Spam

http://www.brightmail.com/spamstats.html

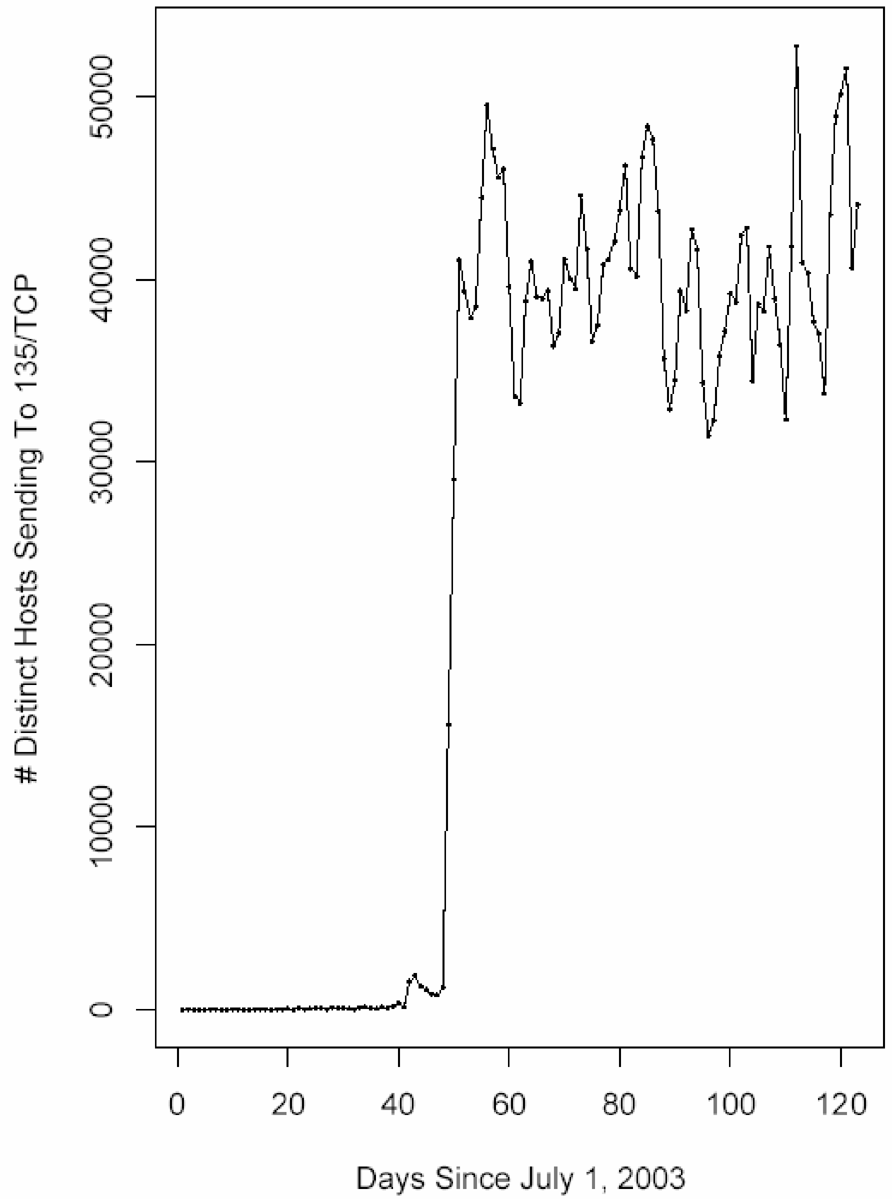


SOURCE: Brightmail Logistics and Operations Center (BLOC)



Source: Xmission Statistics Web Site

Increasing Infectivity Rates

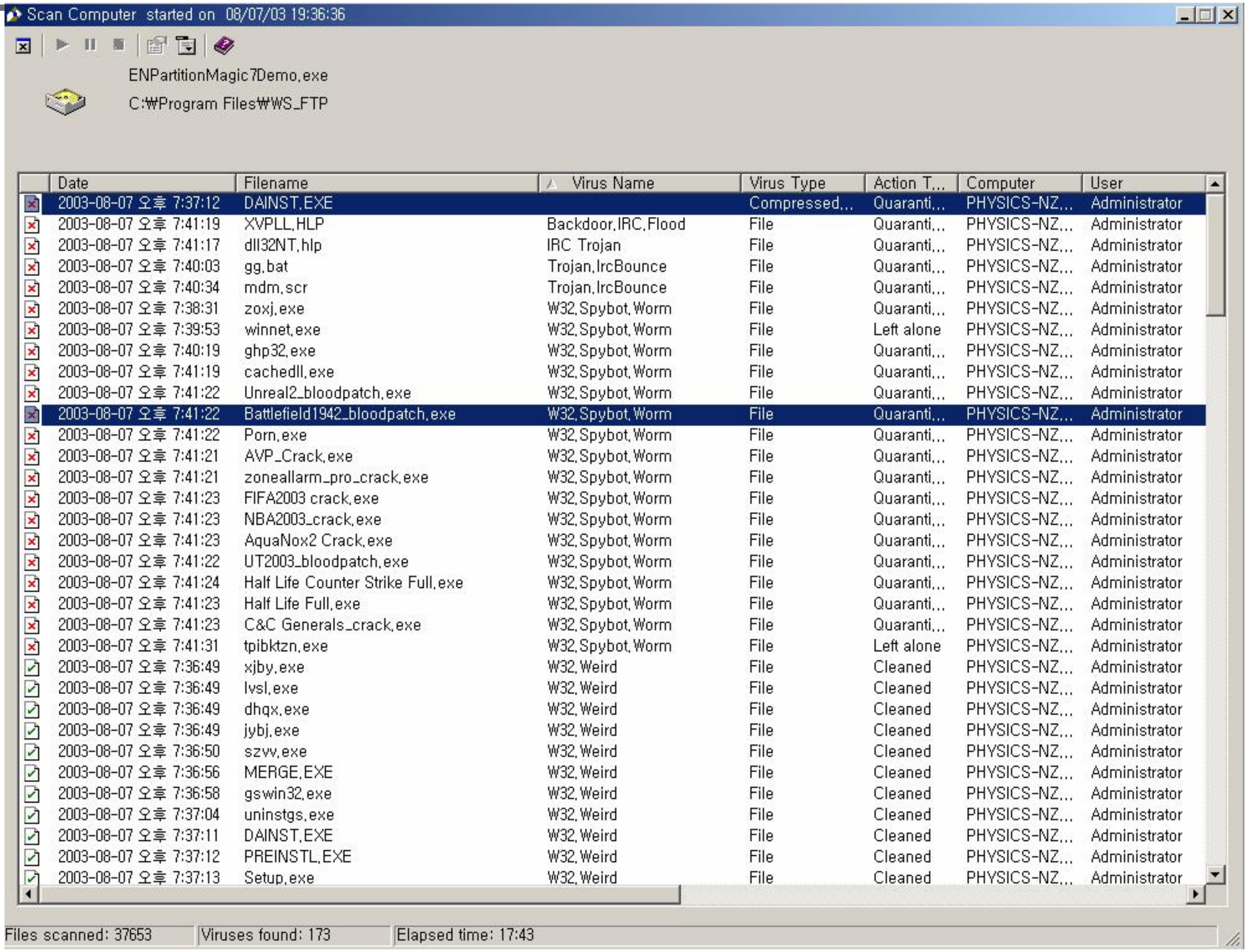


Infectivity Rate:
  Blaster – 1M hosts in 7 days
  Code Red v2: 363,000 hosts in 14 hours
  Slammer: 75,000 hosts in 10 minutes

Its possible that this rate could increase by a further order of magnitude

Source: Vern Paxson

An experimental approach to gathering epidemic infections



Scan Computer started on 08/07/03 19:36:36

ENPartitionMagic7Demo.exe
C:₩Program Files₩WS_FTP

	Date	Filename	Virus Name	Virus Type	Action T...	Computer	User
☒	2003-08-07 오후 7:37:12	DAINST.EXE		Compressed...	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:19	XVPLL.HLP	Backdoor.IRC.Flood	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:17	dll32NT.hlp	IRC Trojan	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:40:03	gg.bat	Trojan.IrcBounce	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:40:34	mdm.scr	Trojan.IrcBounce	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:38:31	zoxj.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:39:53	winnet.exe	W32.Spybot.Worm	File	Left alone	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:40:19	ghp32.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:19	cachedll.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:22	Unreal2_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:22	Battlefield1942_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:22	Porn.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:21	AVP_Crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:21	zoneallarm_pro_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:23	FIFA2003 crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:23	NBA2003_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:23	AquaNox2 Crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:22	UT2003_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:24	Half Life Counter Strike Full.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:23	Half Life Full.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:23	C&C Generals_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
☒	2003-08-07 오후 7:41:31	tpibktzn.exe	W32.Spybot.Worm	File	Left alone	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:49	xjby.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:49	lvsl.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:49	dhqx.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:49	jybj.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:50	szvv.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:56	MERGE.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:36:58	gswin32.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:37:04	uninstgs.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:37:11	DAINST.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:37:12	PREINSTL.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
✓	2003-08-07 오후 7:37:13	Setup.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator

Files scanned: 37653 | Viruses found: 173 | Elapsed time: 17:43

173 (known) viruses
Collected in 17 minutes

(7 Aug 2003)

Why is abuse so effective in the Internet?

- Large population of potential targets
- Significant population of malicious users
- Small (vanishing) marginal cost of use
- Unparallel ability to conceal identity
- Continuing pool of vulnerable systems
- Increasing sophistication of abuse mechanisms
- Potential for rapid dissemination

See: “Trends in Viruses and Worms”, Internet Protocol Journal V6 No3 (www.cisco.com.ipj)

Exploiting the Internet's Strength

- What makes the Internet so compelling is what makes so vulnerable to attack
  - Too good
  - Too fast
  - Too cheap!

What can we expect in the coming years if this continues?

- General spam levels to exceed ‘normal’ mail by factors of up to 100:1 for *everyone*
- Probe traffic volume to exceed ‘normal’ user traffic
- Continued attacks, tending to concentrate on services that attempt to maintain system integrity
- More sophisticated attack forms that attempt to cloak themselves from all forms of automated detection (rapid mutation as a cloaking technique)
- Motivated attacks as distinct from random damage
  - Theft and fraud
  - Deliberate damage and disruption

And our current methods of attacking abuse will fail in the long run…..

- The volume and diversity of attack patterns make traditional method of explicit attack-by-attack filtering completely ineffectual in the face of continued escalation of abuse levels
  - Whatever we are doing today to attempt to identify and isolate abuse traffic will probably not scale up to the expected levels of abuse in 2 – 3 years time
  - A larger, faster, cheaper Internet will simply accelerate abuse patterns
- *So we need to think about different approaches to the problem*

Consequences for the Consumer

- Increasing confusion and alienation regarding the value of Internet services
- Increased suspicion of the ‘trustworthiness’ of the Internet
- Increased total costs of ‘raw’ IP connectivity
- Requirement for increased sophistication of local safeguards

Consequences for ISPs

- Increased level of abuse traffic as a component of the total load
- ISPs are being forced to undertake capacity planning (and infrastructure investment) to operate within the parameter of potential abuse levels, rather than actual use levels
- The full cost of use of Public IP-based services is becoming more expensive for clients, while the perceived benefit is falling

Consequences for all

- The Internet's value proposition is getting worse, not better

What Are the Implications for the Internet Architecture?

- The original end-to-end Internet architecture is under sustained attack
- The end isn't necessarily trustable
- Packet headers are not necessarily trustable
- End-to-End Authentication helpful but not sufficient
  - Capture or subversion of the endpoint may allow the attack vector to masquerade a trusted entity
  - Weaker (but more efficient) authentication may be more useful than strong (but expensive)

What are our Options?

- Denial

  Problem? What Problem?

- Eradication

  Unlikely - so far everything we've done makes it worse!

- Death

  A possible outcome – the value proposition for Internet access declines to the point where users cease using the Internet

- Mitigation

  About all we have left as a viable option

ISP Responses to Abuse

- Do nothing
  - ISPs are common carriers – content is a customer issue
  - Customers can operate whatever firewalls for filters they choose – its not the ISP's business
  - *This is not an effective or sustainable response to the scale of the problem we face here*

ISP Responses to Abuse

- React incident by incident
    - ISP installs traffic filters on their side of a customer connection in response to a customer complaint
    - ISP investigates customer complaints of abuse and attack and attempt to identify the characteristics and sources of the complaint
    - ISP installs filters based on known attacks without a specific customer trigger (permit all, deny some)

    - *This is the common ISP operational procedure in place today*

Is Reaction Enough?

- Its becoming clear that this problem is getting much worse, not better
- In which case specific reaction to specific events is inadequate….
  - Reaction is always after the event.
  - Relies on specific trigger actions
  - Rapid spread implies that delayed response is not enough
  - Does not protect the customer
  - Requires an intensive ISP response
  - Too little, too late

- *This process simply cannot scale*

“Anticipation” of abuse

- Customers only want “good” packets, not “evil” packets
  - And all virus authors ignore RFC 3514!
- It seems that we are being pushed into a new ISP service model:
  - <u>Assume all traffic is hostile, unless explicitly permitted</u>
    - Install filters on all traffic and pass only known traffic profiles to the customer (deny all, permit some)
    - Only permit known traffic profiles from the customer
  - Sounds like a NAT + Firewall?
    - That’s the common way of implementing this today, but it’s not enough

Points of Control

- It looks like the customer-facing edge of the ISP network is becoming the point of application of control mechanisms.
  - Pass traffic to the customer only when:
    - The traffic is part of an active customer-established TCP session, and the TCP session is associated with a known set of explicitly permitted service end-points
    - The traffic is part of a UDP transaction and the session uses known end point addresses

The NAT Model

- NATs fulfill most of these functions:
  - Deny all externally-initiated traffic (probes and disruption attempts)
  - Allow only traffic that is associated with an active internally-initiated session
  - Cloaks the internal persistent identity through use of a common translated address pool

NAT Considerations

- NATs are often criticised because
  - they pervert the end-to-end architectural model
  - they prevent peer-to-peer interaction
  - they represent critical points of failure
  - they prevent the operation of end-to-end security protocols that rely on authenticated headers
  - They complicate other parts of the networked environment (2-faced DNS, NAT ‘agents’, etc)

- BUT
  - maybe we should understand what is driving NAT deployment today and look at why it enjoys such widespread deployment in spite of these considerations

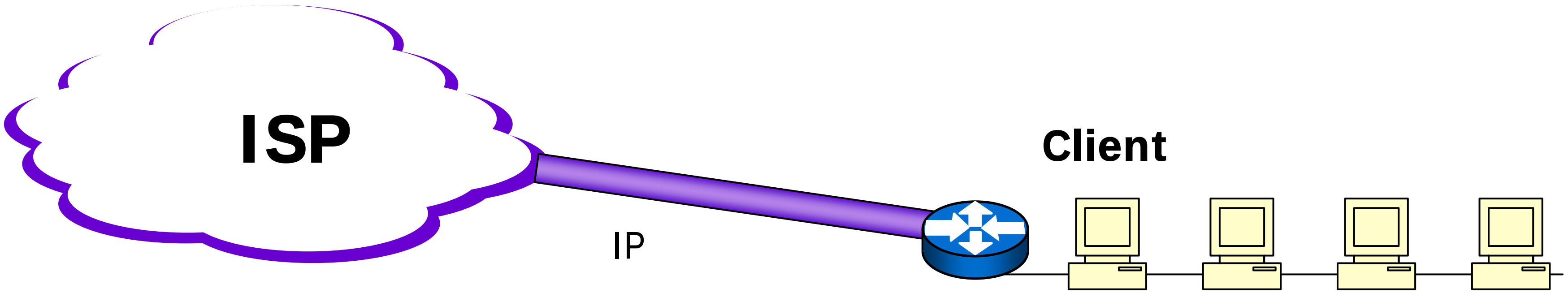
The Generic “Controlled Service” Model

- A ‘Controlled Service’ model:
  - Permit ‘incoming’ traffic only if associated with an established ‘session’ within session state with pre-determined permitted service delivery endpoints
  - Permit outgoing ‘sessions’ according to explicit filters associated with particular service profiles that direct traffic to permitted service delivery endpoints
  - Potential for the service delivery system to apply service-specific filters to the service payload

ISP Service Models

1. The ‘traditional’ ISP Service

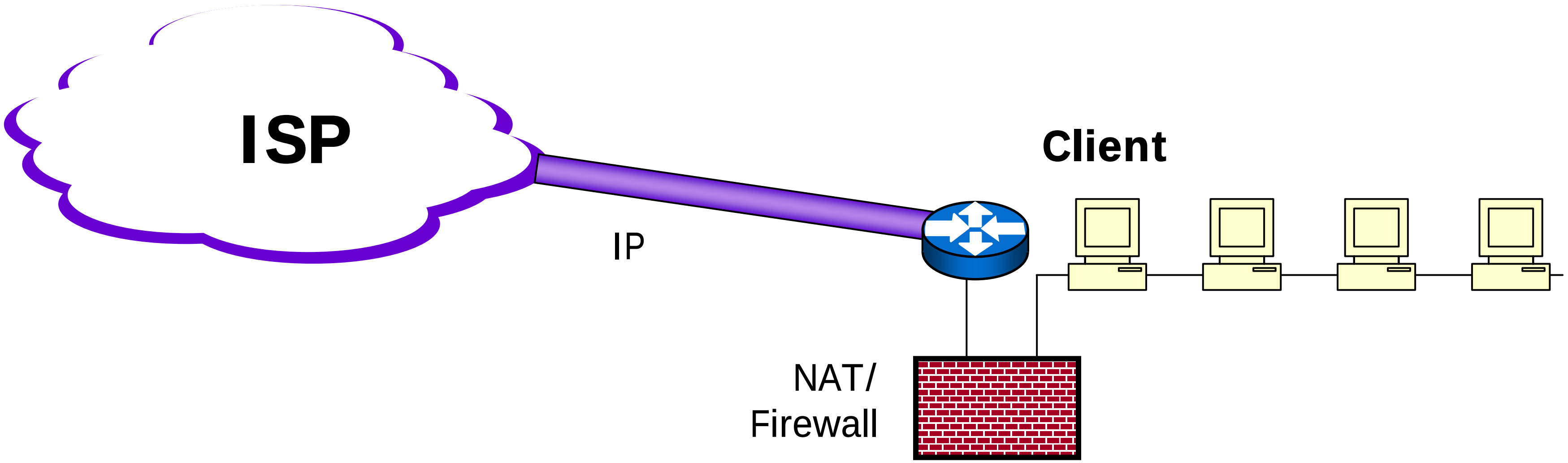
- No common protection mechanism
- Individual hosts fully visible to the Internet



ISP Service Models

2. Customer protection – today's Internet

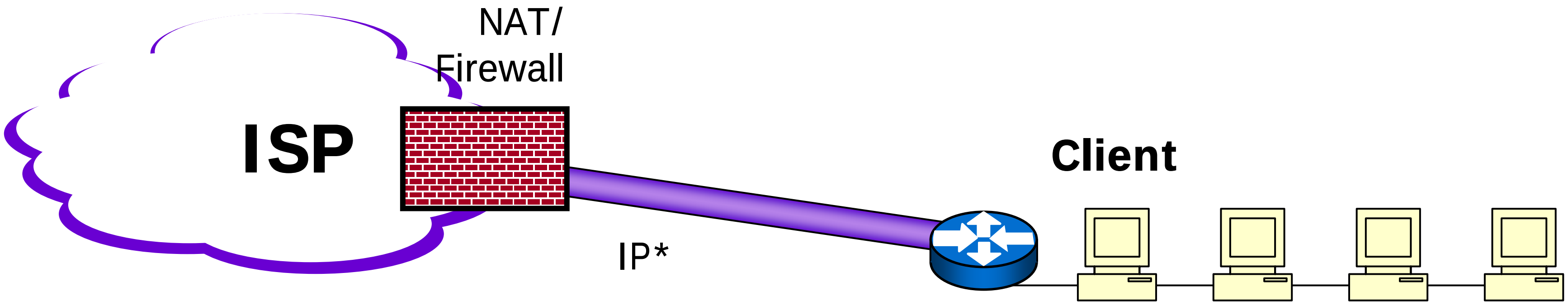
- Customer-installed and operated security system
- All traffic is presented to the customer



ISP Service Models

3. ISP Service Protection – current direction in ISP service architecture

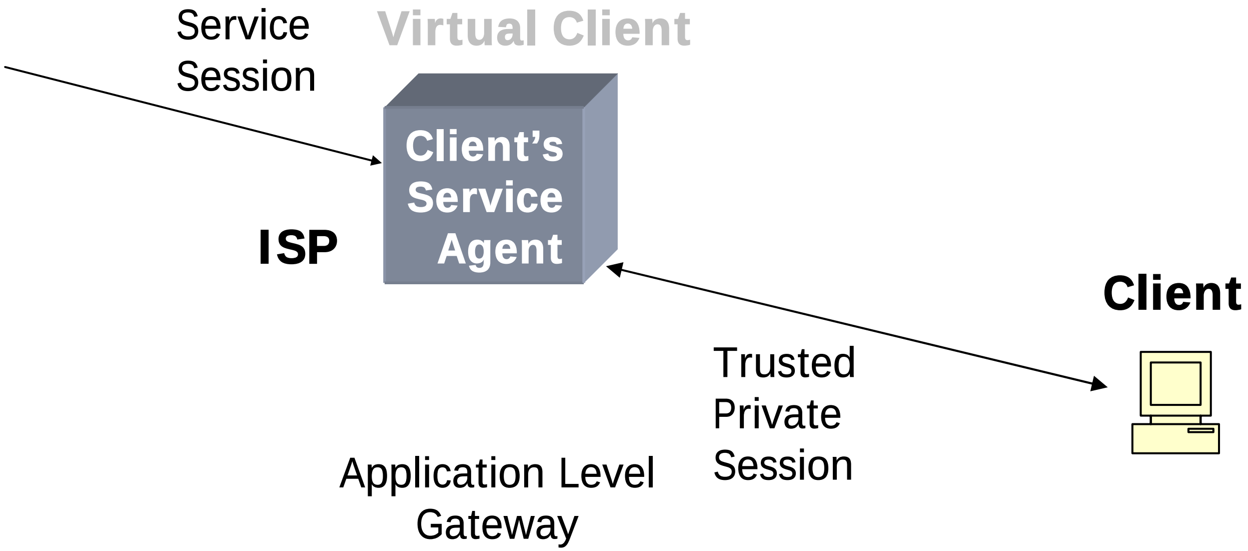
- ISP-installed and operated security system
- Only permitted traffic is presented to the customer



In this model an ISP NAT is dedicated to each client

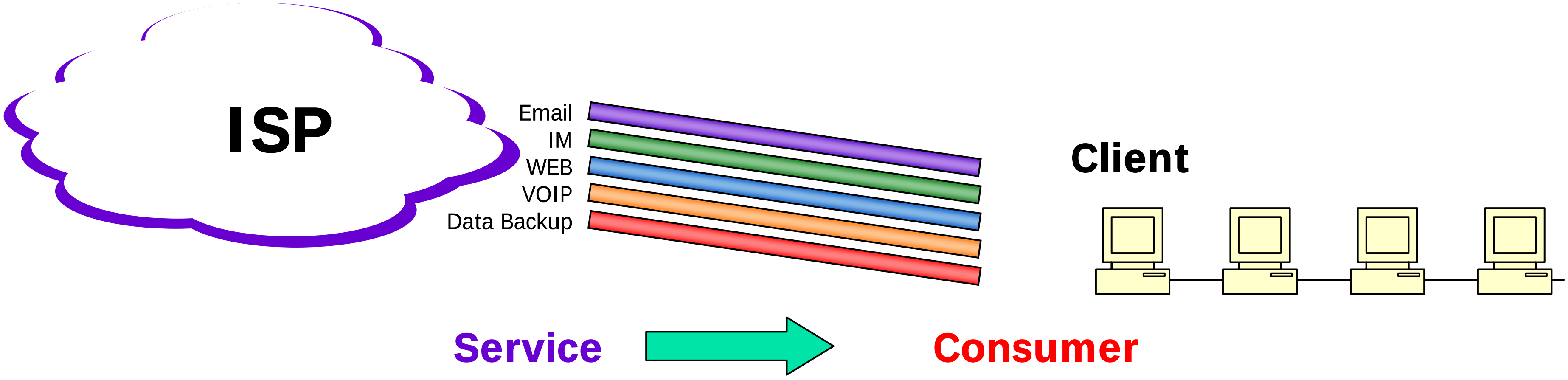
Application Service Implications

- The Virtual Customer Service Model



ISP Implications

- The 'Network Service' model of service provision
  - Move from a peer-to-peer model to a one-way service-consumer model of Internet deployment
  - Services are, once more, **network-centric** rather than **edge-to-edge**



Where is this heading?

- The key direction here is towards deployment of more sophisticated applications that integrate trusted ‘agents’ and brokers and application-specific identity spaces directly into the application framework
  - Keep an eye on SIP as it evolves into more general application rendezvous mechanisms
  - Keep an eye on HIP as it becomes NAT-agile
- The IP layer is probably not the issue any more
  - Control is a service issue, not a Layer 3 issue
  - Coherent global end-to-end IP level addressing may not be a necessary precondition within this form of evolution of service delivery

ISP Positioning

- Does uptake of this service model imply an end to end-to-end IP services?
    - Are we seeing a forced return to a network-centric model of service delivery?
- Is delivery of each service independently contestable?
- Will we see more concentration on service-specific providers with base connectivity infrastructure being further pushed into an undistinguished commodity role?
- Will distinct services evolve to have distinct handling and distinct tariffing?

What’s going on?

- Today’s Internet provides an ideal environment for the spread of abusive epidemics:
  - Large host population
  - Global connectivity
  - Substantial fraction of unprotected hosts
  - Rising infectivity
  - The virus & spam problems are growing at a daunting rate, and to some degree appear interlinked.

Whats the Message?

- There is no cure coming. It will not get better by itself
  - There is no eradicative ‘cure’ for these epidemics – these epidemics will continue to multiply unabated
  - This has implications on customer behaviours and perceived value of service
  - Which in turn has implications on the form of service delivery that customers will value
  - We appear to be heading inexorably away from a ‘raw’ IP peer-to-peer service model into a service/consumer model of network-mediated service delivery

Tomorrow’s ISP

- Will concentrate on reliable trusted SERVICE delivery, not IP connectivity delivery
  - Obviously this shift will imply a number of technology and business implications for the ISP industry, including a return to service-specific delivery mechanisms, network-centric service management and mediation, among other factors.

Maybe…

- The End-to-End model of a simple network with highly functional endpoints and overlay applications is not the optimal model for public services
- Public Services need to operate in a mode that
  - strikes a balance between risk and functionality
  - mediates communications
  - provides network controls for senders and receivers
  - protects vulnerabilities at the edge
- And maybe the answers lie in a better understanding of how services should be delivered across public networks

Discussion?