Smart Network Data Services

Windows Live & MSN Hotmail Postmaster Services

Eliot Gillum

Development Manager, Hotmail and Windows Live Mail

NANOG 37

June 7, 2006

Agenda

- Postmaster Services
- SNDS
  - Problem
  - Goal
  - Today
  - Tomorrow
  - Motivation
  - Feedback / Dialog
  - Questions / Discussion

Postmaster Services

Service	Benefits
Postmaster	▪ Starting point for any questions related to delivering communications to MSN Hotmail and Windows Live consumers
Sender ID	▪ Simple authentication technology that has been adopted by thousands of organizations around the world ▪ Leverages SPF records which have been published by over 1M domains in the world ▪ Virtually eliminates false positives on large sources of legitimate mail ▪ ~85% reduction of false negatives on spoofed mail
Junk Mail Reporting Program (JMRP)	▪ Conveys messages reported by Hotmail and Windows Live accounts ▪ Helps keep internet clean from those who would abuse ISP mail servers ▪ Provides feedback, potentially to be used for opt-out processes, to senders
Smart Network Data Services (SNDS)	▪ Free service that provides data on mail volume, spam, complaints, etc. ▪ Easy online registration and instant access to data ▪ Innovative way to make the Internet a better place!
Support	▪Self-help and escalation paths for senders having deliverability issues

Smart Network Data Services

SNDS

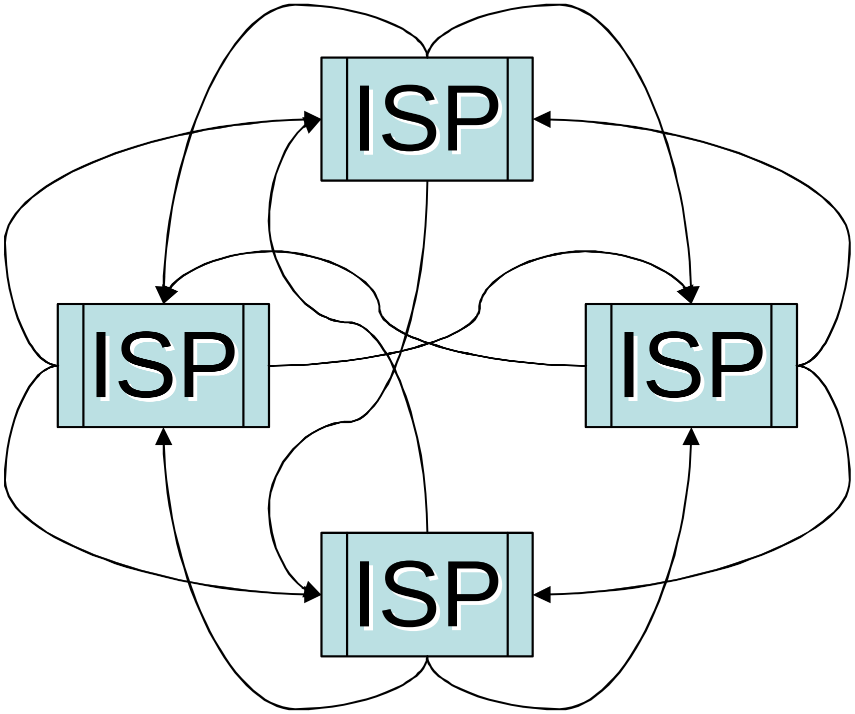
http://postmaster.msn.com/snds

Problem

- Bad stuff on the Internet: spam, phishing, zombies, ID theft, DoS
  - Result: customers unhappy
- Solution #1: Try to stop bad things just before they hit customer
  - Result: progress, learnings
- Solution #2: Apply learnings upstream
  - Result: “game changing” progress!
- **#2:#1 is too low**

ISP-centric Efficiency

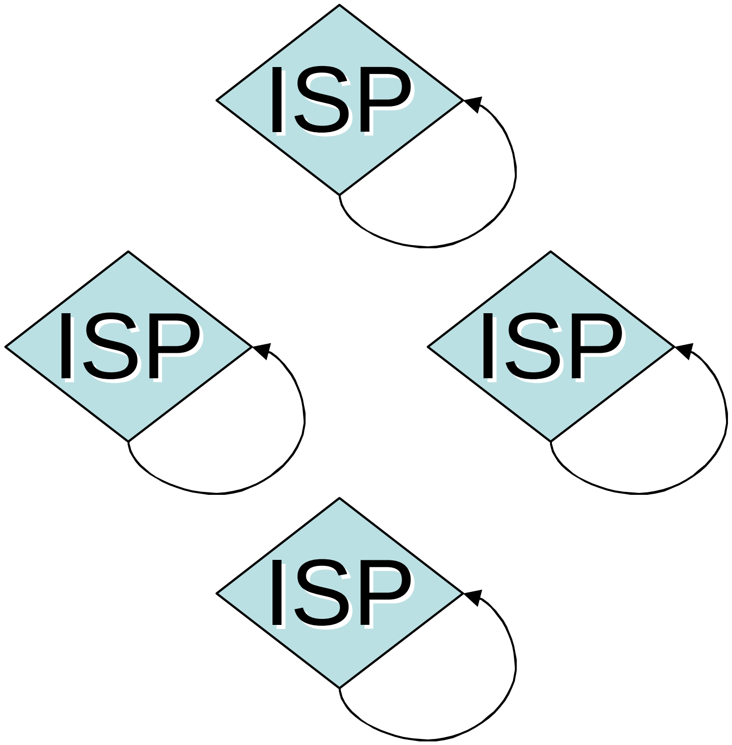
Solution #1



n ISPs have *n-1* problems

→ **O(n^2)**

Solution #2



n ISPs have *1* problem

→ **O(n)**

Crux

- Today people & ISPs are measured by how much bad stuff they *receive*
  - As opposed to what they originate
  - Similarity to the health insurance industry
- "ISPs should monitor their networks for sources of spam LEAVING their network" - Charles Stiles, AOL, NANOG32
- Hutzler to Levine on spam (http://www.circleid.com/posts/how_to_stop_spam/)
  - "The solution is … taking responsibility for … networks being sources of spam"
  - "What do we have to do to persuade networks that dealing with their own spam problem, even at significant short term cost, is better for the net *and themselves* than limping along as we do now?"
- "Machines maintained by home/small-business users are an important aspect of global Internet health" – David Moore, CAIDA, USENIX Sec, Aug '02

7 Step Program

1.	Recognize the problem	SNDS
2.	Believe that someone can help	Me
3.	Decide to do something	You
8.	Make an inventory of those harmed	SNDS
9.	Make amends to them	Tools
10.	Continue to inventory	SNDS
12.	Tell others about the program	You

What is SNDS?

- Website offering free instant access to rich data on activity coming from your IP space as seen by Microsoft
  - Data that correlates with “Internet evils”
  - Informs ISP to enable local policy decisions
- Automated authorization mechanism
  - Uses WHOIS and rDNS
  - Users are people not companies
- A *force multiplier*

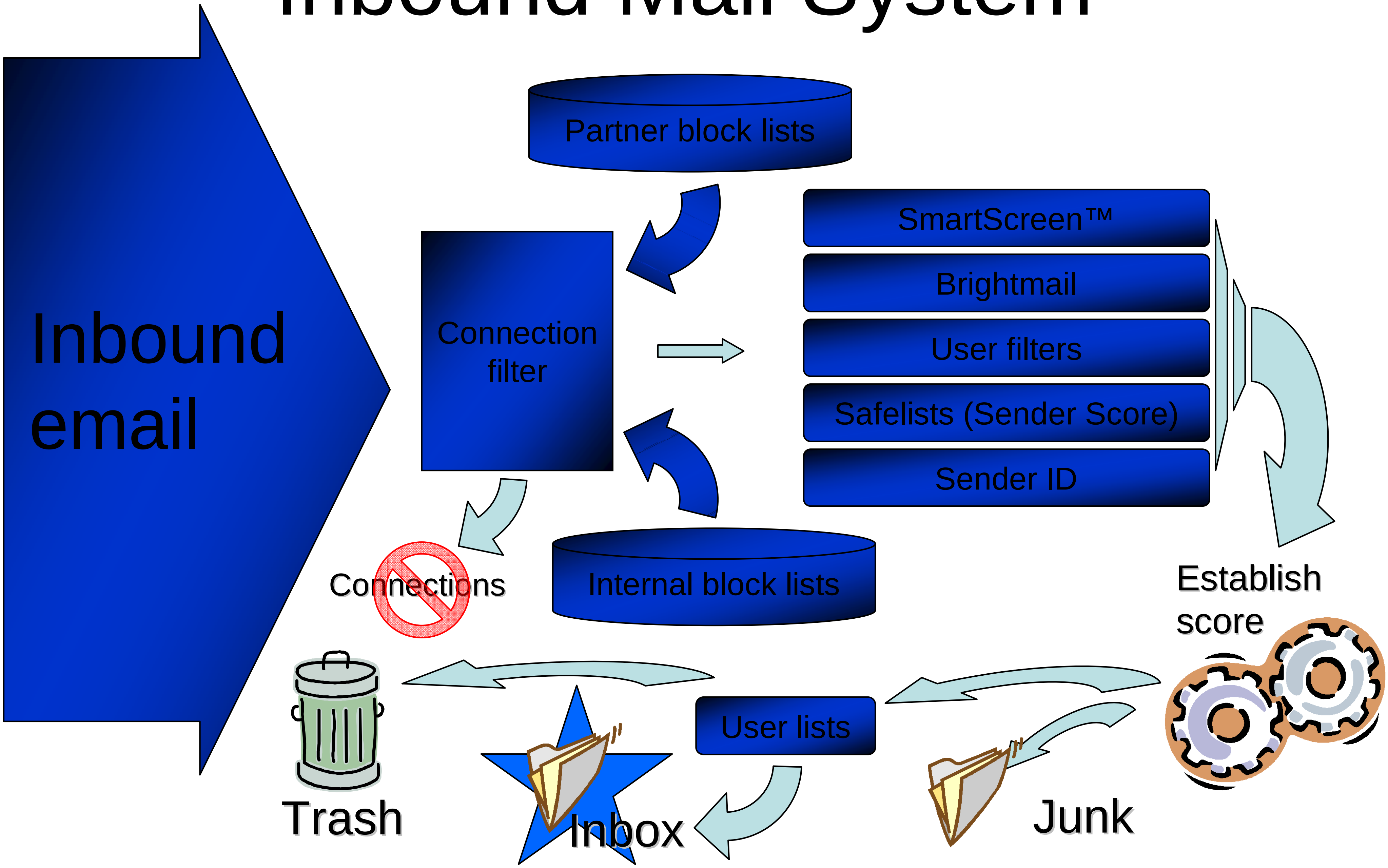
SNDS Goal

- Provide information which enables ISPs to monitor for and remediate any undesired activity
  - Qualitative and quantitative data
    - Factual, actionable information about email sent to us and, by extension, to the world in general
- "No ISP left behind"
- Stop problems upstream of the destination
  - Evangelize virtues of doing so
- Bring TCR down to absolute minimum
- Make the Internet a better, safer place

We Have Data

- Windows Live Mail / MSN Hotmail is a spam and spoofing target
  - 240+ million accounts in over 220 countries/territories
- Many kinds of data
  - 4 billion inbound mails/day
    - 90/10 spam/ham by filtering technologies
  - User reports on:
    - Spam
    - Fraud
  - Phishing
  - Viruses
  - Malware
- Reporting tools across Microsoft
  - Windows Live / MSN Hotmail web UI
  - Internet Explorer
  - MSN Toolbar
  - Outlook Express Live

Inbound Mail System



Inbound email

Partner block lists

Connection filter

SmartScreen™

Brightmail

User filters

Safelists (Sender Score)

Sender ID

Connections

Internal block lists

Establish score

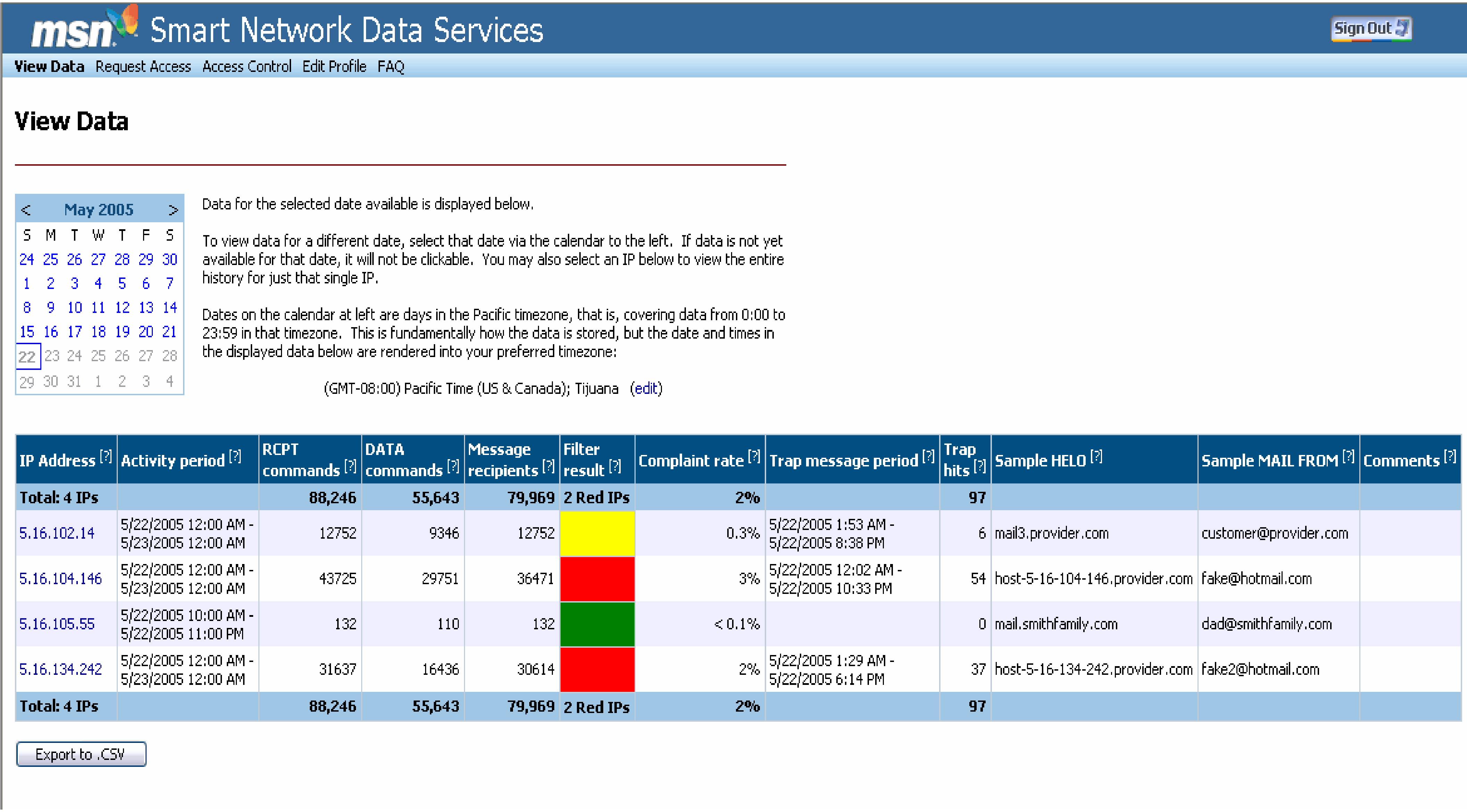
User lists

Trash

Inbox

Junk

SNDS Today



View Data

<			May 2005			>
S	M	T	W	T	F	S
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Data for the selected date available is displayed below.

To view data for a different date, select that date via the calendar to the left. If data is not yet available for that date, it will not be clickable. You may also select an IP below to view the entire history for just that single IP.

Dates on the calendar at left are days in the Pacific timezone, that is, covering data from 0:00 to 23:59 in that timezone. This is fundamentally how the data is stored, but the date and times in the displayed data below are rendered into your preferred timezone:

(GMT-08:00) Pacific Time (US & Canada); Tijuana (edit)

IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 4 IPs		**88,246**	**55,643**	**79,969**	**2 Red IPs**	**2%**		**97**			
5.16.102.14	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	12752	9346	12752	🟨	0.3%	5/22/2005 1:53 AM - 5/22/2005 8:38 PM	6	mail3.provider.com	customer@provider.com	
5.16.104.146	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	43725	29751	36471	🟥	3%	5/22/2005 12:02 AM - 5/22/2005 10:33 PM	54	host-5-16-104-146.provider.com	fake@hotmail.com	
5.16.105.55	5/22/2005 10:00 AM - 5/22/2005 11:00 PM	132	110	132	🟩	< 0.1%		0	mail.smithfamily.com	dad@smithfamily.com	
5.16.134.242	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	31637	16436	30614	🟥	2%	5/22/2005 1:29 AM - 5/22/2005 6:14 PM	37	host-5-16-134-242.provider.com	fake2@hotmail.com	
Total: 4 IPs		**88,246**	**55,643**	**79,969**	**2 Red IPs**	**2%**		**97**			

Today’s Scenarios

- Illustrate magnitude and *evidence* of problem
  - Additional resources
  - Monitoring infrastructure
- Spam
  - Enact port 25 blocking
    - Justify classical blocks
    - Enable reactive “surgical” blocks
- Work with the customer!
  - Notify them
  - Help them
  - Motivate them

SNDS Stats

- 2500 users
  - Mostly “senders”
- 67 Million IPs
- 10-20% of inbound mail & complaints

- **Output drops by 57% on /24+ when monitored via SNDS**

SNDS Tomorrow*

- Usability
  - Signup by ASN
  - Better support for upstream providers
  - Access transfer
- Utility
  - Programmatic access
- Data
  - Virus-infected emails
  - Phishing
  - HoneyMonkey
  - Sample messages

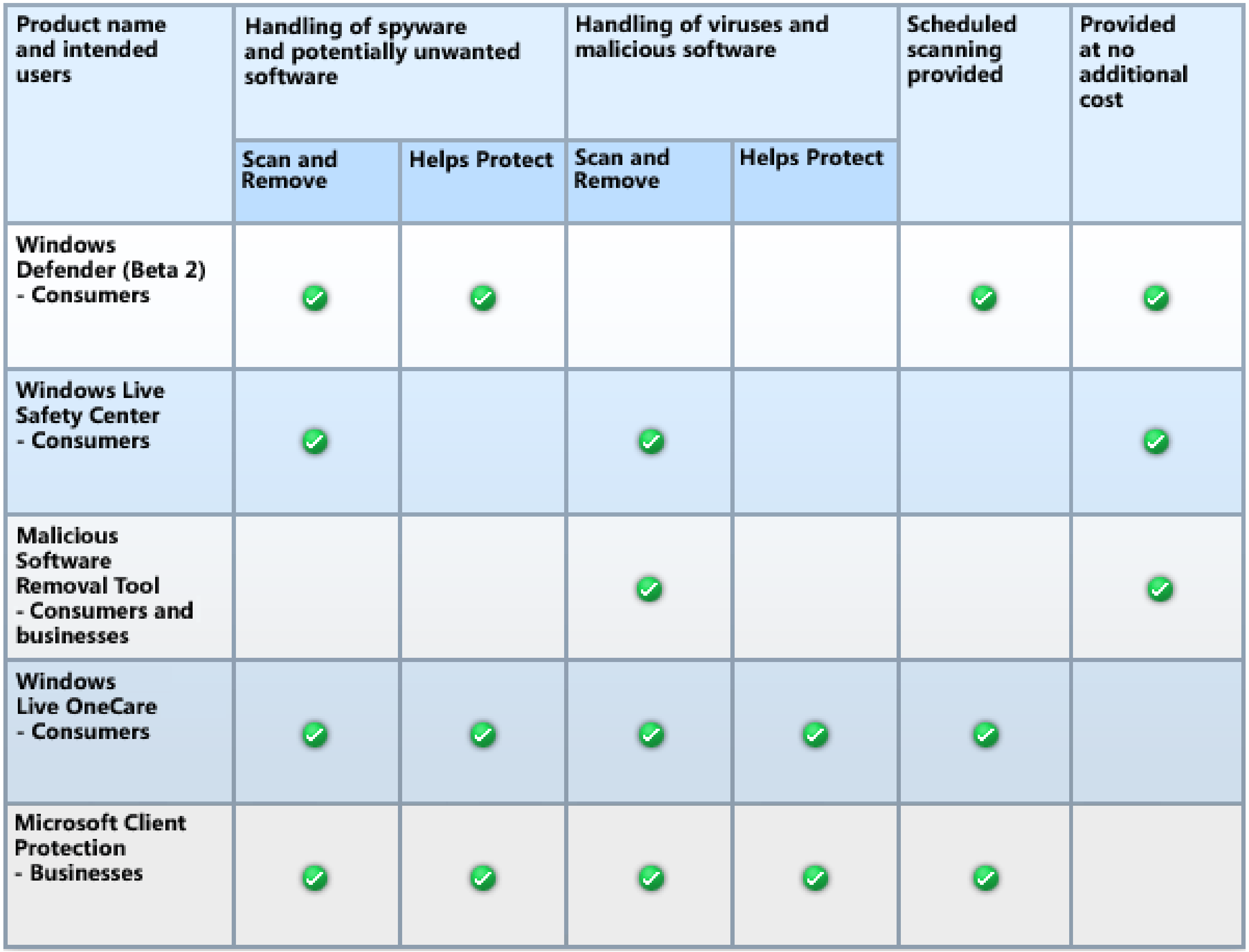
Tomorrow’s Scenarios

- Lowered
  - – Barrier to entry
  - – Recurring “cost”
- ISP types
  - – End-user
  - – Tier 1/2 monitoring tier 2/3
- Directly attack more than just spam
  - – Virus emails → infected PCs, outbound virus filters
  - – Phishing/malware hosting → take-downs

Safety Tools

- Stinger http://vil.nai.com/vil/stinger/
- Nessus http://www.nessus.org/
- Windows Update http://update.microsoft.com/
- Windows Defender
- Malicious Software Removal Tool
- Windows Live Safety Center http://safety.live.com
- Windows OneCare http://www.windowsonecare.com/
- Phishing Filter Add-in for MSN Toolbar http://addins.msn.com/phishingfilter/
  - Also built into Internet Explorer 7

Safety Tools



Product name and intended users	Handling of spyware and potentially unwanted software		Handling of viruses and malicious software		Scheduled scanning provided	Provided at no additional cost
	Scan and Remove	Helps Protect	Scan and Remove	Helps Protect		
Windows Defender (Beta 2) - Consumers	✓	✓			✓	✓
Windows Live Safety Center - Consumers	✓		✓			✓
Malicious Software Removal Tool - Consumers and businesses			✓			✓
Windows Live OneCare - Consumers	✓	✓	✓	✓	✓	
Microsoft Client Protection - Businesses	✓	✓	✓	✓	✓	

Motivation

Hypothesis: everyone benefits

- Customers
  - Infected users get fixed
  - Safer, cheaper, better Internet experience
- ISPs
  - Solution #1 isn’t *solving* the problem
  - Altruistic is the “new” selfish
- Microsoft
  - Only benefits if everyone else does

ISP Motivation

- Customers
  - They’re unhappy, unsafe
  - They like people who fix that
    - Be the hero
    - Retain customers
    - Win new ones
  - Fixing has more benefit than bandaging
- Cost reductions
  - Bandwidth
  - Support
- Community
  - NANOG?

Motivation Alternatives

- Industry scorecard
  - Public recognition
  - Public shame
- Logo ISP program
- Government: Legislation / Regulation
  - “[FTC Chairman Deborah Platt Majoras] emphasized the importance of information sharing” – Press Release, Oct ’04 http://www.ftc.gov/opa/2004/10/spamconference.htm

Business Case

- “Industry attention at the ISP level is now concentrating on product marketing aspects of the Internet service model: Dependability, Integrity, Value-add”
  - Geoff Huston, APNIC, NANOG 35
- Appeal to cost reduction and *revenue generation*
  - Marketing: Safety makes customers happy
  - Sales: Safety has revenue sharing potential
  - Operations & Support: Safety reduces costs
- This is starting to happen
  - “Automatically Detecting, Isolating, and Cleaning Infected Hosts”
    - Eric Gauthier, Boston University, NANOG 30

Feedback

- Usability – how easily can you work with it?
- Utility – what are you able to accomplish?
- What’s missing?
  - Tools to aid customer remediation

- How do ISPs see cost vs. benefits?
  - Costs, benefits, NANOG aggregation?
- How do we get to critical mass?

- msn-snds@microsoft.com

Discussion

- How does SNDS fit into the larger ecosystem?
  - Relationship to:
    - SenderBase.org
    - SCOMP / JMRP
    - REACT
  - Should / how do other ISPs provide this?
    - Common schema, authorization, authentication
    - Federation, delegation, aggregation

- Forum
  - BoF? Track?
  - NANOG? MAAWG?
  - Mailing list: upstream@mipassoc.org

Conclusion

- Postmaster: http://postmaster.msn.com
  - Start page: JMRP, support, Sender ID, and…
- SNDS: http://postmaster.msn.com/snds
  - **Try it!**
    - **Tell your friends**
    - Tell your boss
    - Stay tuned
  - Tell us what happened!
  - What comes next?

Authorization Mechanism

- Based on being able to receive mail at a “trusted” email address
- Address determination
  - Reverse DNS
    - If all the IPs in the range are in the same “domain”, then trust the standard mailboxes, postmaster and abuse, at that domain
    - “Domain” determined by largest known TLD plus one more hostname component
    - Range must be less than /23 in size
  - WHOIS
    - Trust any addresses that appear in the most specific WHOIS record for the range

SenderID Key Results

- SIDF with reputation improves filtering
  - Legitimate, SIDF-compliant mail realizes a substantial reduction in false-positives
    - Improves deliverability and resulting open rates
    - High volume ‘good’ senders who publish, their false positives has essentially dropped to zero
  - False negatives on fail (implying spoofing) is ~85% lower than a random sampling of non-SIDF mail
    - Improving brand and customer protection
- Business value, improving deliverability while reducing false positives and false negatives with reputation
- http://www.microsoft.com/senderid/