Regional Development Forum 2008

“Bridging the Standardization Gap in Developing Countries” for the Asia-Pacific Region

Hanoi, Vietnam, 15-17(am) September 2008

- Improving Internet Security: Australia’s Spam and BotNet initiatives

- **Mick Owens,**
- **Manager, International Section**
- **Australian Communications and Media Authority**

Spam, botnets & cybersecurity

- Spam the vector for substantial number of compromised computers
- More than 90 per cent of worldwide spam sent from botnets – vast majority ‘criminal’ spam
- Worldwide spam continues to increase – large increase in second half of 2007
- Botnets and spam closely interrelated
- Addressing bots and botnets will reduce spam and enhance cybersecurity

Cybercrime trends in the first half of 2008

- Some current trends:
  - Emails are less likely to contain malware – but instead promote links to compromised websites with stories on celebrities or current events as ‘bait’
  - Website infection rates are three times greater than in 2007
  - Over 90 per cent of webpages spreading Trojan horses and spyware are legitimate websites (hacked by SQL injection)
  - Web 2.0 networking sites have introduced new risks
  - New examples of suspicious software received by security firms about every four seconds

Economic drivers for combating botnets

- 67% of Australian internet users aged 18 years and over use the internet, for banking, shopping or bill payment (May 2008) *ACMA (unpublished/ unweighted data)*
- 8.2 million Australians aged 16 years and older (equivalent to 52% of the Australian population) have used online banking (April 2007) *Commonwealth Bank E-Money Survey*
- Critical that consumer confidence in using the internet for commercial transactions is maintained/enhanced
- Potential for erosion of confidence in usage of internet for transactions if e-security environment worsens, with significant economic impact

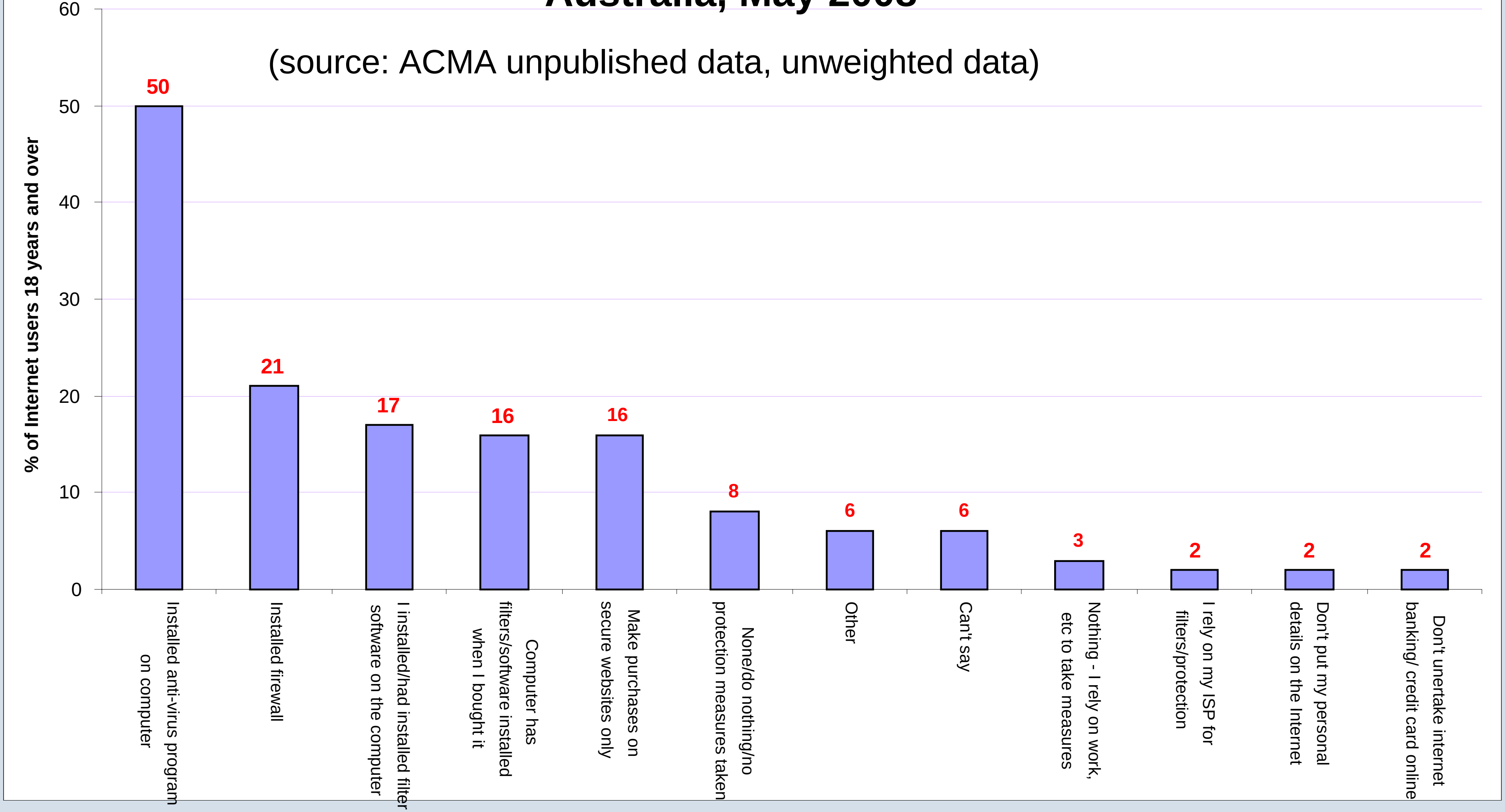
Economic drivers for criminals

- Low cost operation for criminals
- Relatively low risk – prosecutions complex – investigations require extensive international cooperation
- Highly profitable
- Unwariness of public – June 2008 Australian Bureau of Statistics survey found Australians lost $AU977 million to personal fraud in the12 months prior to interview - 453,100 victims lost money
  - Method of fraud includes by internet, telephone/mobile, post or in person

Australian Government

Australian Communications and Media Authority

Protective measures used to reduce online risks, Australia, May 2008



(source: ACMA unpublished data, unweighted data)

Australian integrated strategy to combat spam

1. Strong enforcement
2. Education and awareness activities
3. Industry measures
4. **Technological initiatives and solutions**
5. International cooperation

Similar integrated approach required to combat botnets

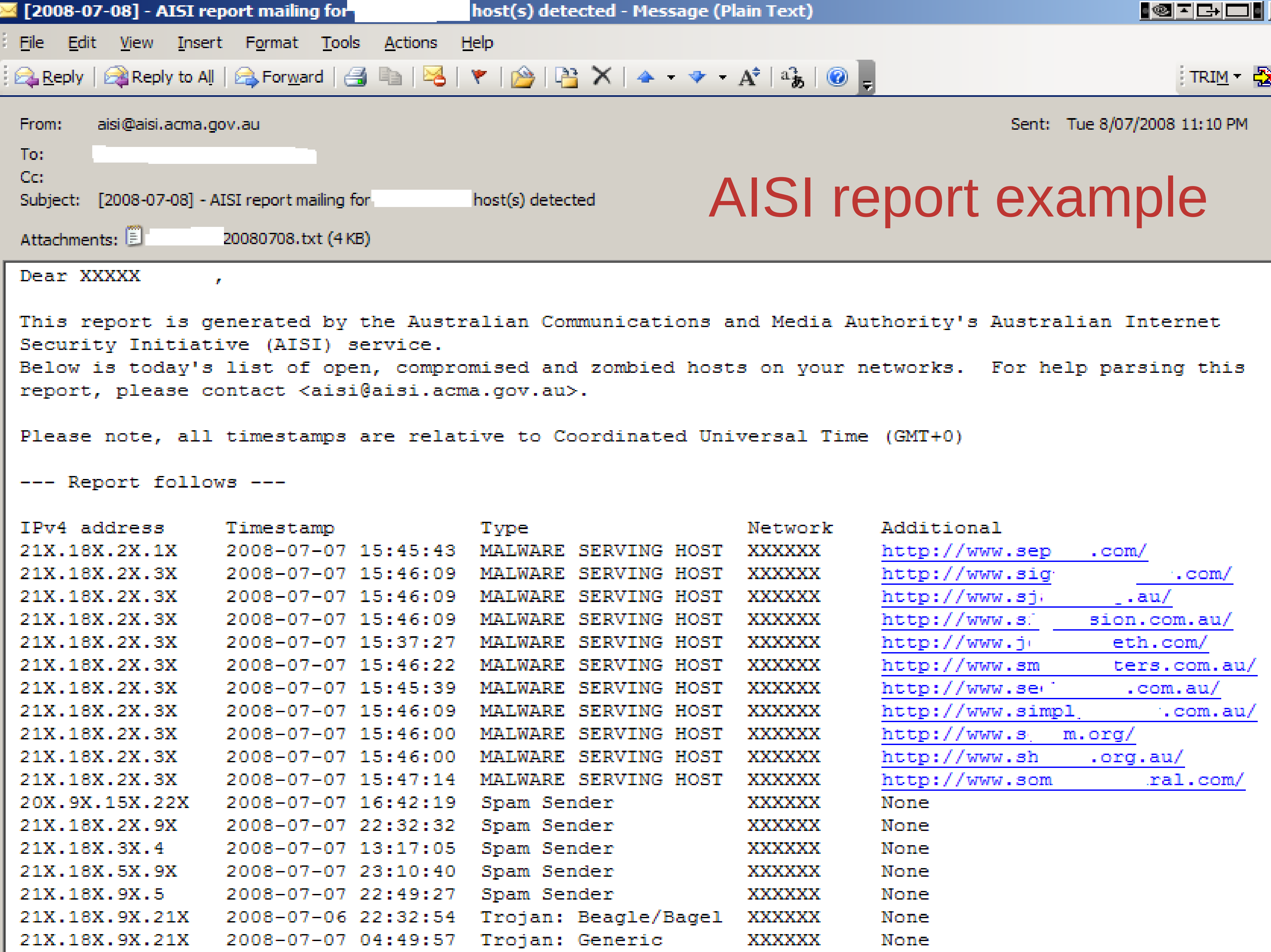
Australian Internet Security Initiative (AISI)

- Pilot of AISI commenced in November 2005 – six internet service providers (ISPs) involved
- Pilot assessed in 2006 and found to be of merit
- Funding for enhancement/expansion of AISI provided by Australian Government in 2007
- Progressively developed since that time
- Currently 52 ISPs participating

What is the AISI?

- Daily reports provided by email to ISPs identifying ‘compromised’ IP addresses on their networks
- Compromise must have been identified in 24 hour period prior to the report
- Report contains IP address and time stamp for compromise
- ISPs correlate the IP address to their customer logs to identify the customer associated with IP address
- ISPs contact customer and advise of infection and provide advice on how to fix problem

AISI report example


[2008-07-08] - AISI report mailing for [redacted] host(s) detected - Message (Plain Text)
File
Edit
View
Insert
Format
Tools
Actions
Help
Reply
Reply to All
Forward
TRIM

From: aisi@aisi.acma.gov.au

Sent: Tue 8/07/2008 11:10 PM

To: [redacted]

Cc:

Subject: [2008-07-08] - AISI report mailing for [redacted] host(s) detected

Attachments: [redacted]20080708.txt (4 KB)

```
Dear XXXXX [redacted],

This report is generated by the Australian Communications and Media Authority's Australian Internet
Security Initiative (AISI) service.
Below is today's list of open, compromised and zombied hosts on your networks.  For help parsing this
report, please contact <aisi@aisi.acma.gov.au>.

Please note, all timestamps are relative to Coordinated Universal Time (GMT+0)

--- Report follows ---

IPv4 address     Timestamp            Type                 Network    Additional
21X.18X.2X.1X    2008-07-07 15:45:43  MALWARE SERVING HOST XXXXXX     http://www.sep[redacted].com/
21X.18X.2X.3X    2008-07-07 15:46:09  MALWARE SERVING HOST XXXXXX     http://www.sig[redacted].com/
21X.18X.2X.3X    2008-07-07 15:46:09  MALWARE SERVING HOST XXXXXX     http://www.sj[redacted].au/
21X.18X.2X.3X    2008-07-07 15:46:09  MALWARE SERVING HOST XXXXXX     http://www.s[redacted]sion.com.au/
21X.18X.2X.3X    2008-07-07 15:37:27  MALWARE SERVING HOST XXXXXX     http://www.j[redacted]eth.com/
21X.18X.2X.3X    2008-07-07 15:46:22  MALWARE SERVING HOST XXXXXX     http://www.sm[redacted]ters.com.au/
21X.18X.2X.3X    2008-07-07 15:45:39  MALWARE SERVING HOST XXXXXX     http://www.se[redacted].com.au/
21X.18X.2X.3X    2008-07-07 15:46:09  MALWARE SERVING HOST XXXXXX     http://www.simpl[redacted].com.au/
21X.18X.2X.3X    2008-07-07 15:46:00  MALWARE SERVING HOST XXXXXX     http://www.s[redacted]m.org/
21X.18X.2X.3X    2008-07-07 15:46:00  MALWARE SERVING HOST XXXXXX     http://www.sh[redacted].org.au/
21X.18X.2X.3X    2008-07-07 15:47:14  MALWARE SERVING HOST XXXXXX     http://www.som[redacted]ral.com/
20X.9X.15X.22X   2008-07-07 16:42:19  Spam Sender          XXXXXX     None
21X.18X.2X.9X    2008-07-07 22:32:32  Spam Sender          XXXXXX     None
21X.18X.3X.4     2008-07-07 13:17:05  Spam Sender          XXXXXX     None
21X.18X.5X.9X    2008-07-07 23:10:40  Spam Sender          XXXXXX     None
21X.18X.9X.5     2008-07-07 22:49:27  Spam Sender          XXXXXX     None
21X.18X.9X.21X   2008-07-06 22:32:54  Trojan: Beagle/Bagel XXXXXX     None
21X.18X.9X.21X   2008-07-07 04:49:57  Trojan: Generic      XXXXXX     None
```

ACMA interaction with AISI ‘customers’

- ACMA does not know which customers have been identified as compromised unless the customer is referred to ACMA by their ISP or the ISP contacts ACMA on their behalf
- Customers more likely to contact ACMA if they have been identified as having a ‘malware serving host’ compromise
- Almost all queries about ‘false positives’ have been proven to be accurate reports

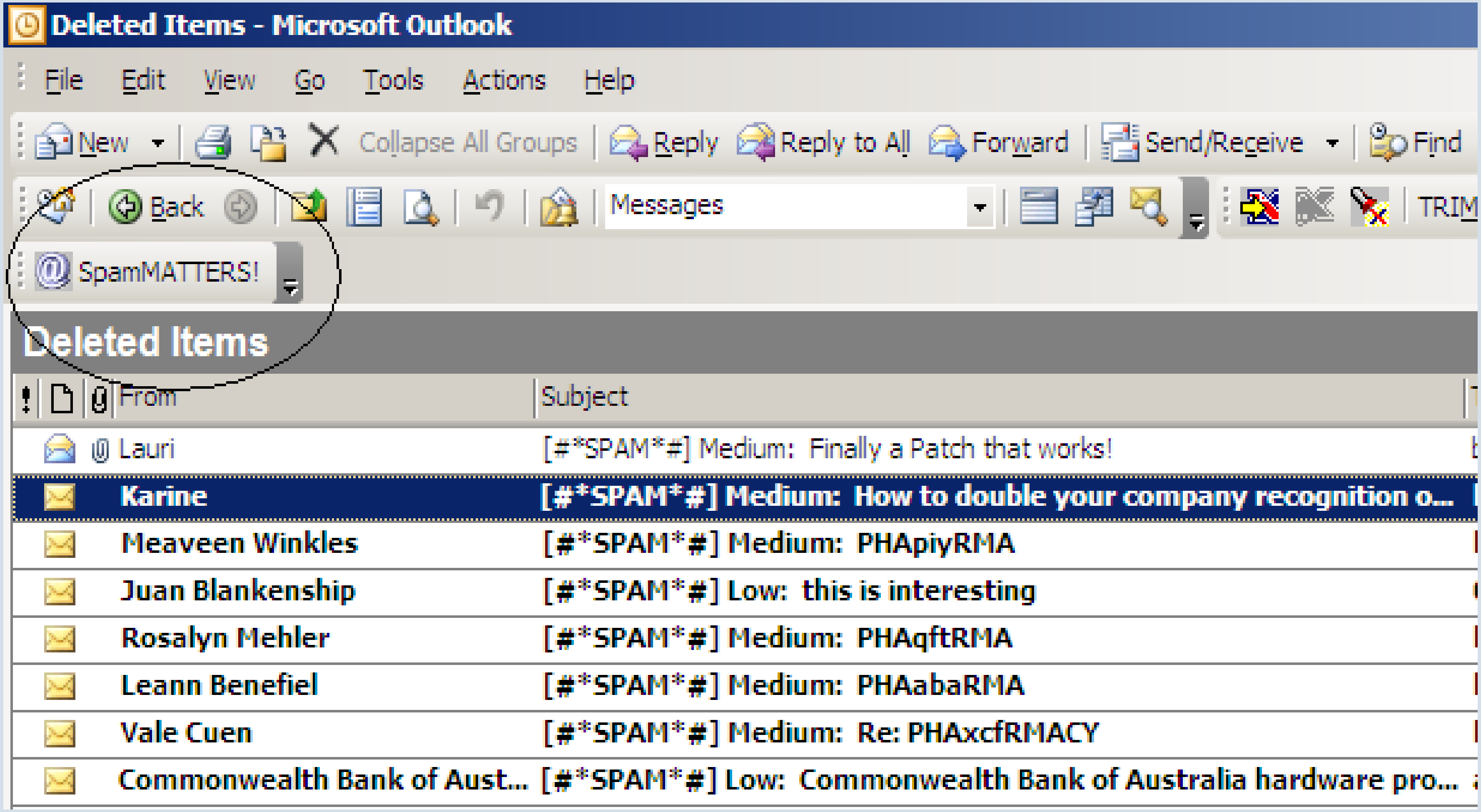
AISI trends and statistics

- Estimated 90 per cent of Australian home internet users covered
- Currently over 3000 compromises reported daily
- Equates to more that 1,000,000 reports per annum
- ACMA is working to enhance the AISI both in terms of features and data feeds

Enhancements to AISI

- Recent advances
  - Provision of additional data on compromises
  - Prioritisation of data (i.e. ‘malware serving hosts’) identified - requested by some ISPs
- Potential future advances
  - Establishment of ISP forum for sharing information on e-security
  - Development of portal where ISPs can download AISI data & information
  - Adding ‘seen before’ advice if same IP address recently compromised
  - Expansion of data sources

SpamMATTERS – Reporting Button



From	Subject
Lauri	[#*SPAM*#] Medium: Finally a Patch that works!
Karine	[#*SPAM*#] Medium: How to double your company recognition o...
Meaveen Winkles	[#*SPAM*#] Medium: PHApiyRMA
Juan Blankenship	[#*SPAM*#] Low: this is interesting
Rosalyn Mehler	[#*SPAM*#] Medium: PHAqftRMA
Leann Benefiel	[#*SPAM*#] Medium: PHAabaRMA
Vale Cuen	[#*SPAM*#] Medium: Re: PHAxcfRMACY
Commonwealth Bank of Aust...	[#*SPAM*#] Low: Commonwealth Bank of Australia hardware pro...

AISI relationship to other e-security initiatives

- AISI part of e-Security National Agenda – Securing Australia’s Online Environment (ESNA)
- Closely linked to other Government initiatives aimed at enhancing the protection of home users and small to medium to enterprises
- A number of Australian Government agencies involved
- Whole of Government review of Australia’s e-security arrangements announced on 2 July 2008
- Further information at: www.ag.gov.au/esecurityreview
- Also www.staysmartonline.gov.au

International cooperation: spam & e-security

- Sharing information on ‘best-practice’ to aid cross border enforcement helps improving security and regulatory responses to spam and e-security threats
- A key group in the Asia-Pacific region is the Seoul-Melbourne (anti-spam) MOU Group
- Currently includes 13 members from 10 jurisdictions
  - More information available at: www.sm-mou.org/
- New members from the region are welcome
- Another key group is the London Action Plan
  - More information at: www.londonactionplan.org/

International cooperation: spam & e-security

- The AISI model could be applied elsewhere
  - The ITU is developing a Botnet Toolkit that is 'inspired' by the AISI
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf

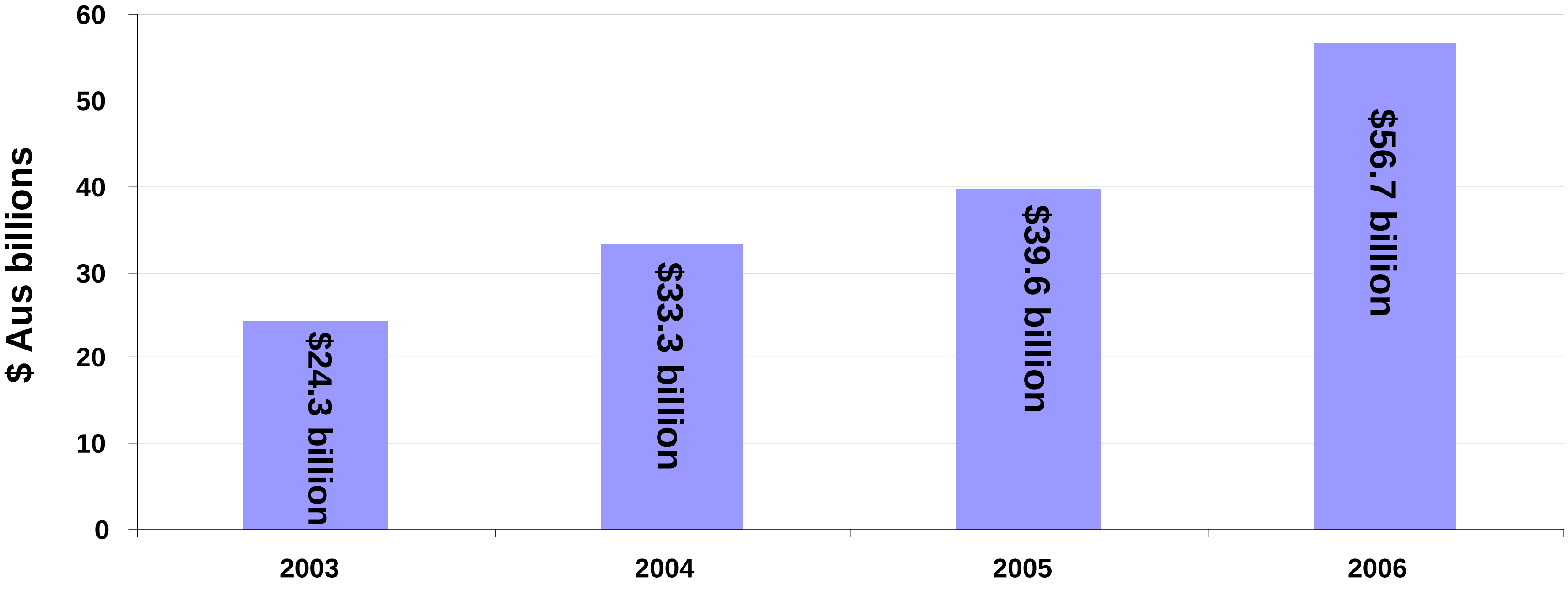
- Enquiries on the AISI welcome at: aisi@aisi.acma.gov.au

Thank you

Australian Government
Australian Communications and Media Authority

The internet and the Australian economy

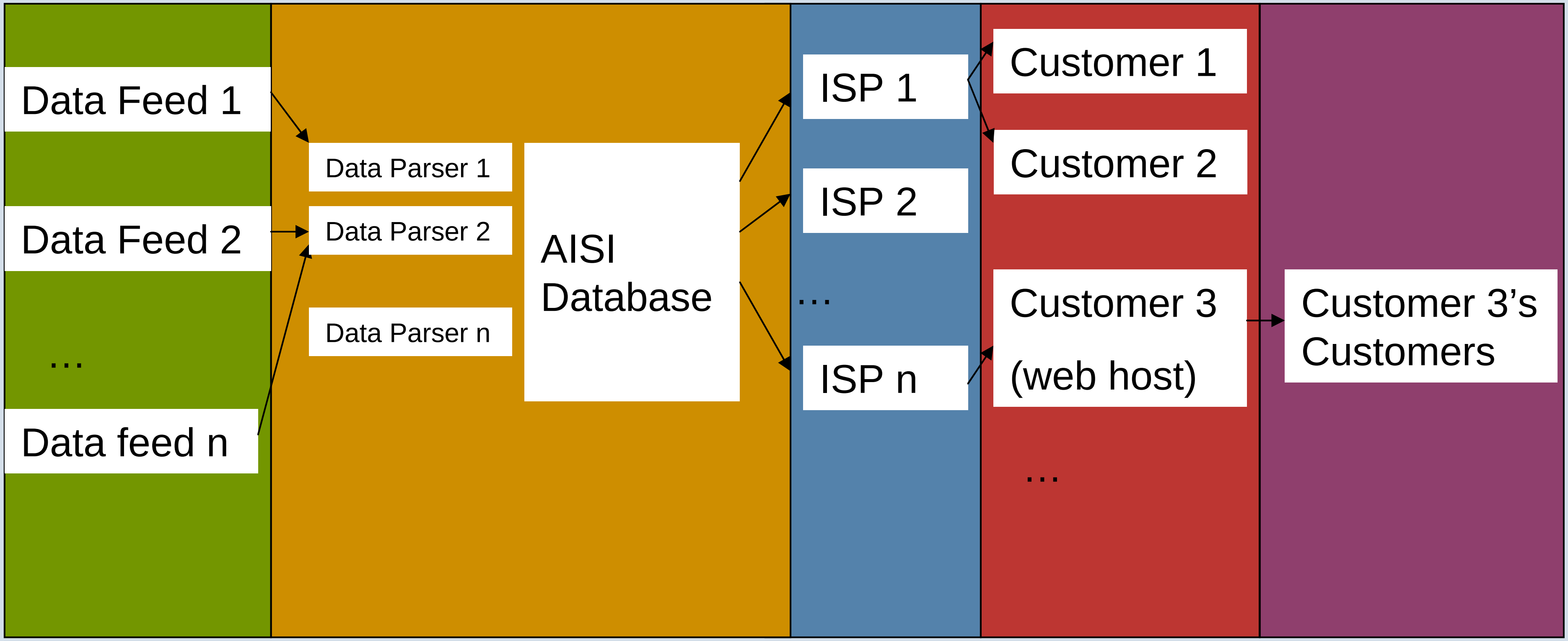
Value of Internet e-commerce* (Aus $. Source: ABS)



Financial year ending June

* e-commerce=selling goods or services online

AISI Process Flow



Data Feed 1

Data Feed 2

…

Data feed n

Data Parser 1

Data Parser 2

Data Parser n

AISI Database

ISP 1

ISP 2

…

ISP n

Customer 1

Customer 2

Customer 3 (web host)

…

Customer 3's Customers