Australian Government
Australian Communications and Media Authority

Australia's regulator for broadcasting, the internet, radiocommunications and telecommunications

www.acma.gov.au

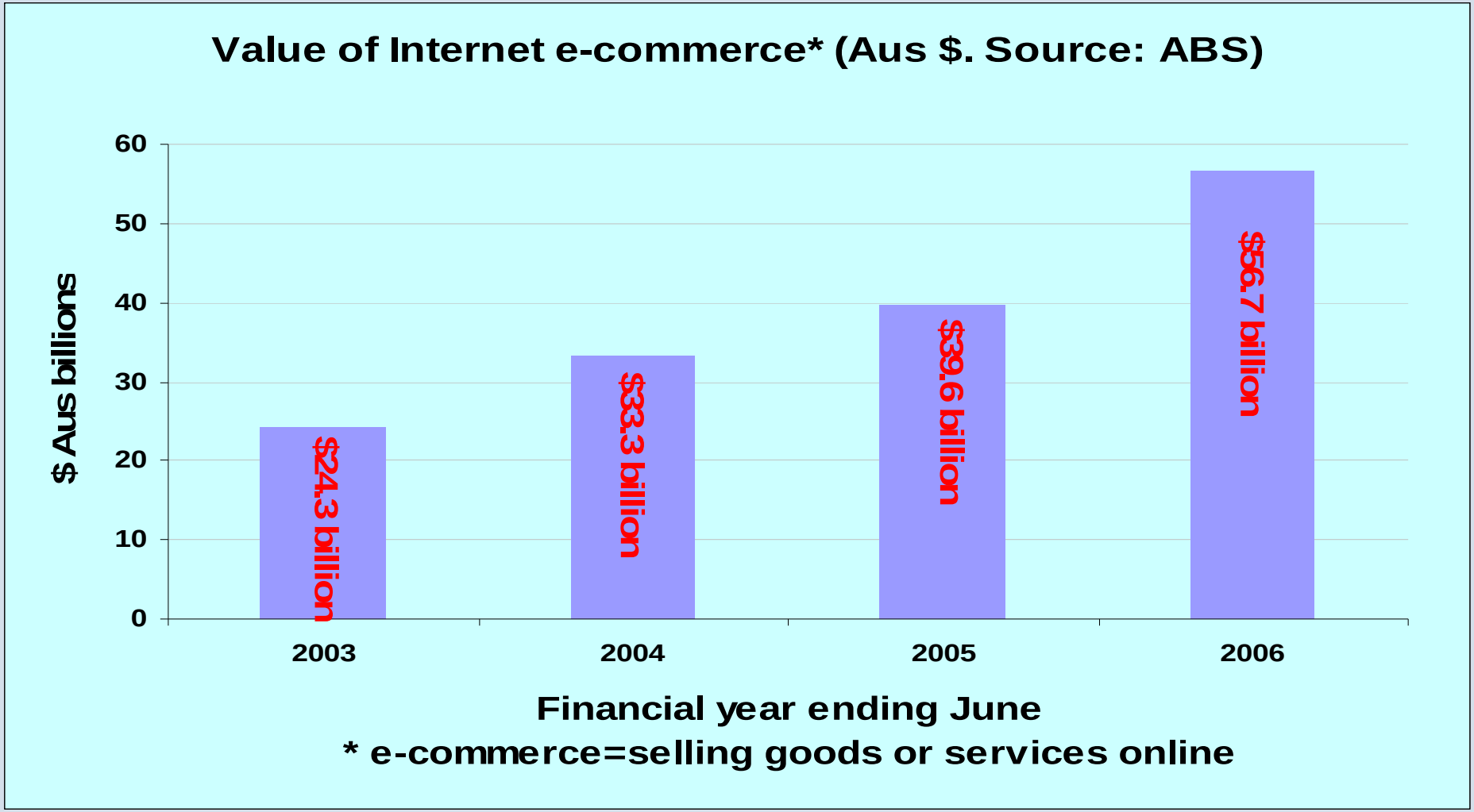
Australia's Spam and Zombie Initiatives: Economic Drivers

ITU Seminar on the Economics of Cybersecurity
Brisbane, Australia
15 July 2008

Bruce Matthews
Manager, Anti-Spam Team

Australian Government
Australian Communications and Media Authority

The internet and the Australian economy



Australian Government
Australian Communications and Media Authority

Australian internet usage ubiquitous

- 13.2 million Australians aged 14 years and over are estimated to have used the Internet
- 10.9 million in the last week before being surveyed

  (Roy Morgan Single Source, May 2008)
- In terms of media consumption - Australians spending more time online than watching television (Nielsen Online – March 2008)

Australian Government
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

Australian Government
Australian Communications and Media Authority

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internet users aged 18 years and over use the internet, for banking, shopping or bill payment (May 2008) *ACMA (unpublished/ unweighted data)*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

Australian Government
Australian Communications and Media Authority

Economic drivers for criminals

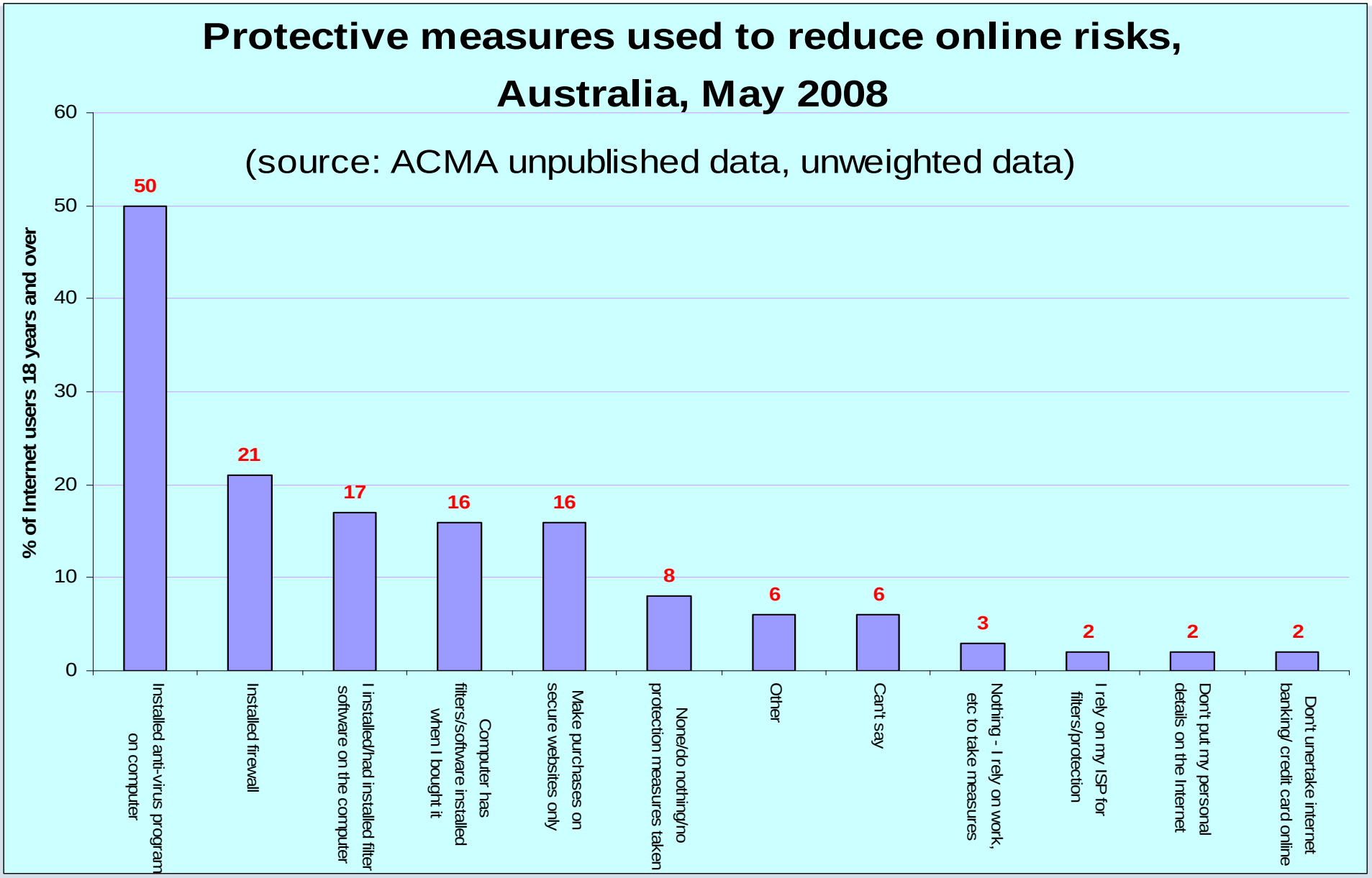
- Low cost operation for criminals
- Relatively low risk – prosecutions complex – investigations require extensive international cooperation
- Highly profitable
- Unwariness of public – June 2008 Australian Bureau of Statistics survey found Australians lost $AU977 million to personal fraud in the12 months 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)



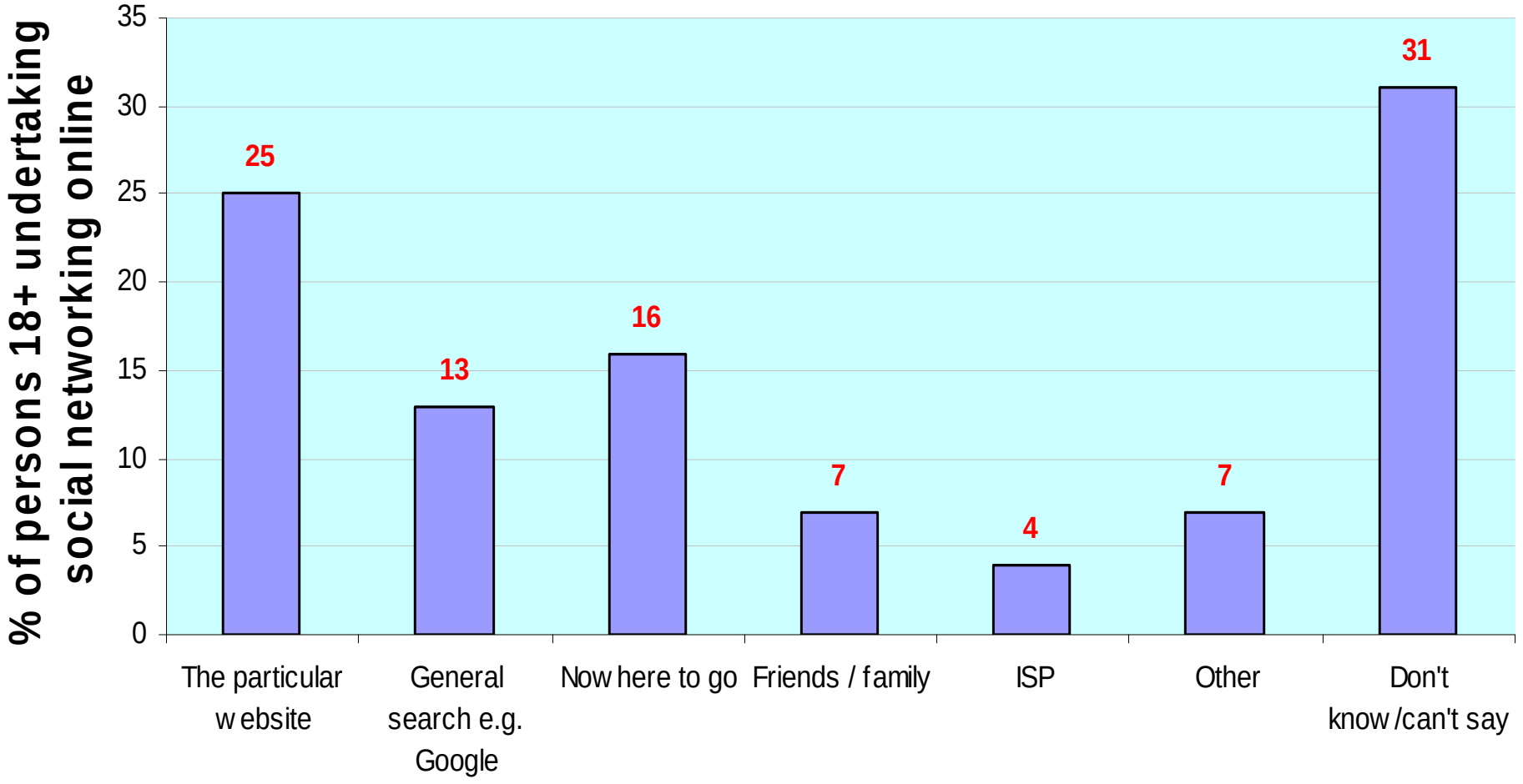
Australian Government
Australian Communications and Media Authority

Comments on ACMA 'protective measures' data

- Indicates a significant proportion of users do nothing or take minimal protective measures when using the internet
- These internet users particularly susceptible to becoming part of a botnet
- Indicates need to increase awareness in Australia of importance of protective measures when using the internet
- Recent June 2008 e-security awareness week (including launch of national alert service) part of ongoing awareness raising activities
- Data will form part of a future detailed ACMA report

Australian Government
Australian Communications and Media Authority

Where would you go for information about how to protect your personal details from possible misuse? [Question asked of users of social networking sites]
(ACMA unpublished data May 2008 unweighted)



Australian Government
Australian Communications and Media Authority

Personal information protection challenges

- Almost half of respondents said they either had either ‘nowhere to go’ or weren’t sure of where to go for information on protecting their personal details
- Highlights the need to promote authoritative information sources
- Further ACMA market material at http://www.acma.gov.au/WEB/STANDARD/pc=PC_9058

Australian Government
Australian Communications and Media Authority

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 Government
Australian Communications and Media Authority

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 38 ISPs participating

Australian Government
Australian Communications and Media Authority

AISI ISP participation list

- AAPT
- Access Net Pty Ltd
- AOL
- AUSTARnet
- Bekkers
- Central Data
- Chariot
- Comcen
- Dodo Australia
- Dreamtilt
- Global Dial
- Grapevine
- Highway 1
- Hotkey
- iiNet
- Internode
- IntraPower
- iPrimus
- Neighbourhood Cable
- Netspace
- Nextep
- OneWire
- Optus Internet
- Pacific Internet (Australia)
- Reynolds Technology
- Riverland Internet
- Soul Communications
- Speedweb Internet
- Spin Internet
- Telstra Bigpond
- TPG Internet
- TSN Communications
- Uecomm
- Unwired
- West Australian Networks
- Westnet
- Wideband Networks

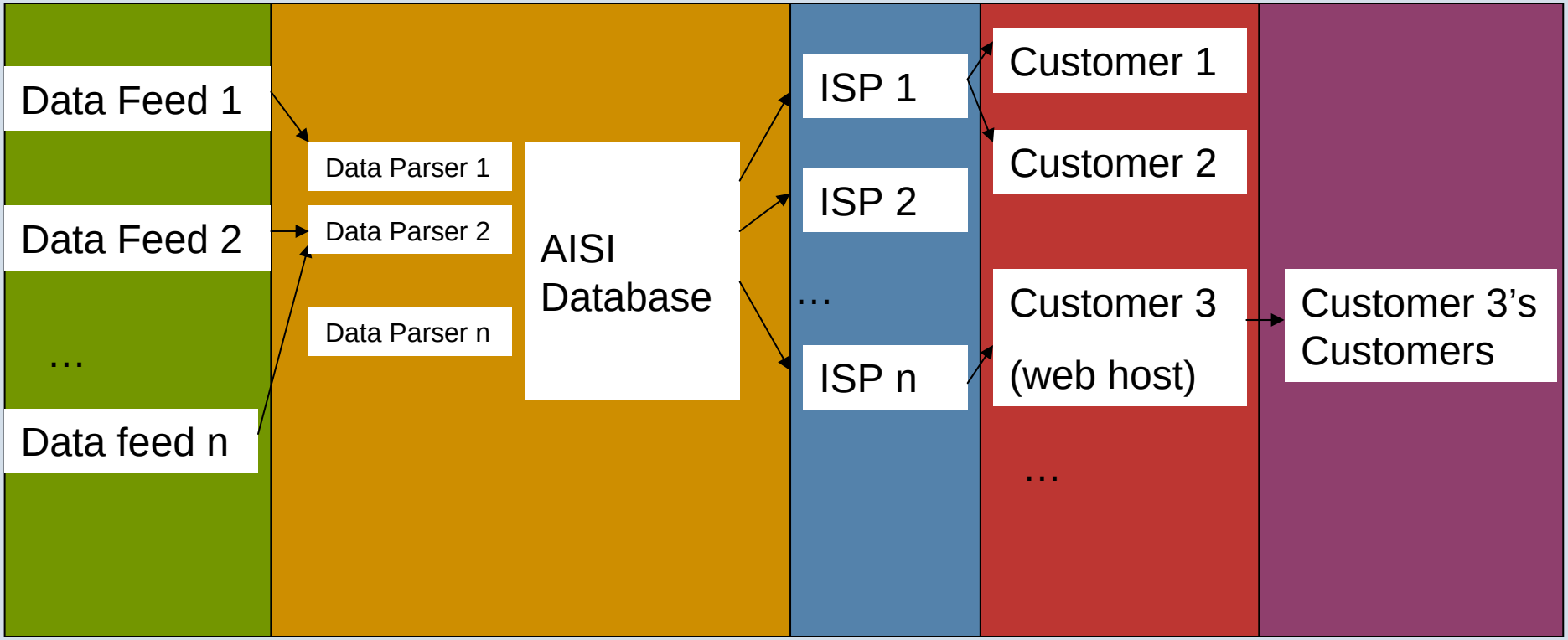
Australian Government
Australian Communications and Media Authority

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

Australian Government
Australian Communications and Media Authority

AISI Process Flow



[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)

AISI report example

Dear XXXXX ,

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 .com/
21X.18X.2X.3X	2008-07-07 15:46:09	MALWARE SERVING HOST	XXXXXX	http://www.sig .com/
21X.18X.2X.3X	2008-07-07 15:46:09	MALWARE SERVING HOST	XXXXXX	http://www.sj .au/
21X.18X.2X.3X	2008-07-07 15:46:09	MALWARE SERVING HOST	XXXXXX	http://www.s sion.com.au/
21X.18X.2X.3X	2008-07-07 15:37:27	MALWARE SERVING HOST	XXXXXX	http://www.j eth.com/
21X.18X.2X.3X	2008-07-07 15:46:22	MALWARE SERVING HOST	XXXXXX	http://www.sm ters.com.au/
21X.18X.2X.3X	2008-07-07 15:45:39	MALWARE SERVING HOST	XXXXXX	http://www.se .com.au/
21X.18X.2X.3X	2008-07-07 15:46:09	MALWARE SERVING HOST	XXXXXX	http://www.simpl .com.au/
21X.18X.2X.3X	2008-07-07 15:46:00	MALWARE SERVING HOST	XXXXXX	http://www.s m.org/
21X.18X.2X.3X	2008-07-07 15:46:00	MALWARE SERVING HOST	XXXXXX	http://www.sh .org.au/
21X.18X.2X.3X	2008-07-07 15:47:14	MALWARE SERVING HOST	XXXXXX	http://www.som 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

Australian Government
Australian Communications and Media Authority

AISI trends and statistics

- Estimated 90 per cent of home internet users covered
- 3060 compromises currently reported daily to ISPs (average over 1 April to 30 June 2008)
- Equates to more that 1,000,000 reports per annum

Australian Government
Australian Communications and Media Authority

Critical roles of ISPs in AISI

- ISPs contact customer through different methods, according to their specific circumstances: telephone, automated email, integration with ‘abuse’ reporting system, written correspondence
- AISI strongly supported by peak internet industry bodies: including Internet Industry Association and Western Australian Internet Association – promote AISI to members
- Detailed survey of ISPs to be conducted in late 2008

Australian Government
Australian Communications and Media Authority

ACMA interaction with AISI 'customers'

- ACMA does not know which ISP's customers have been identified as compromised unless….
  - customer with compromise referred to ACMA by ISP or ISP contacts ACMA on their behalf
- Customer contact has increased significantly since 'malware serving host' compromise category introduced
- Most queries about 'false positives' have been proven to be accurate reports – however, there are occasional false positives, as in the following example
  - ' we are running a newsletter server on this IP address… Our typical mail outs are in order of 100,000 to 500,000 emails'

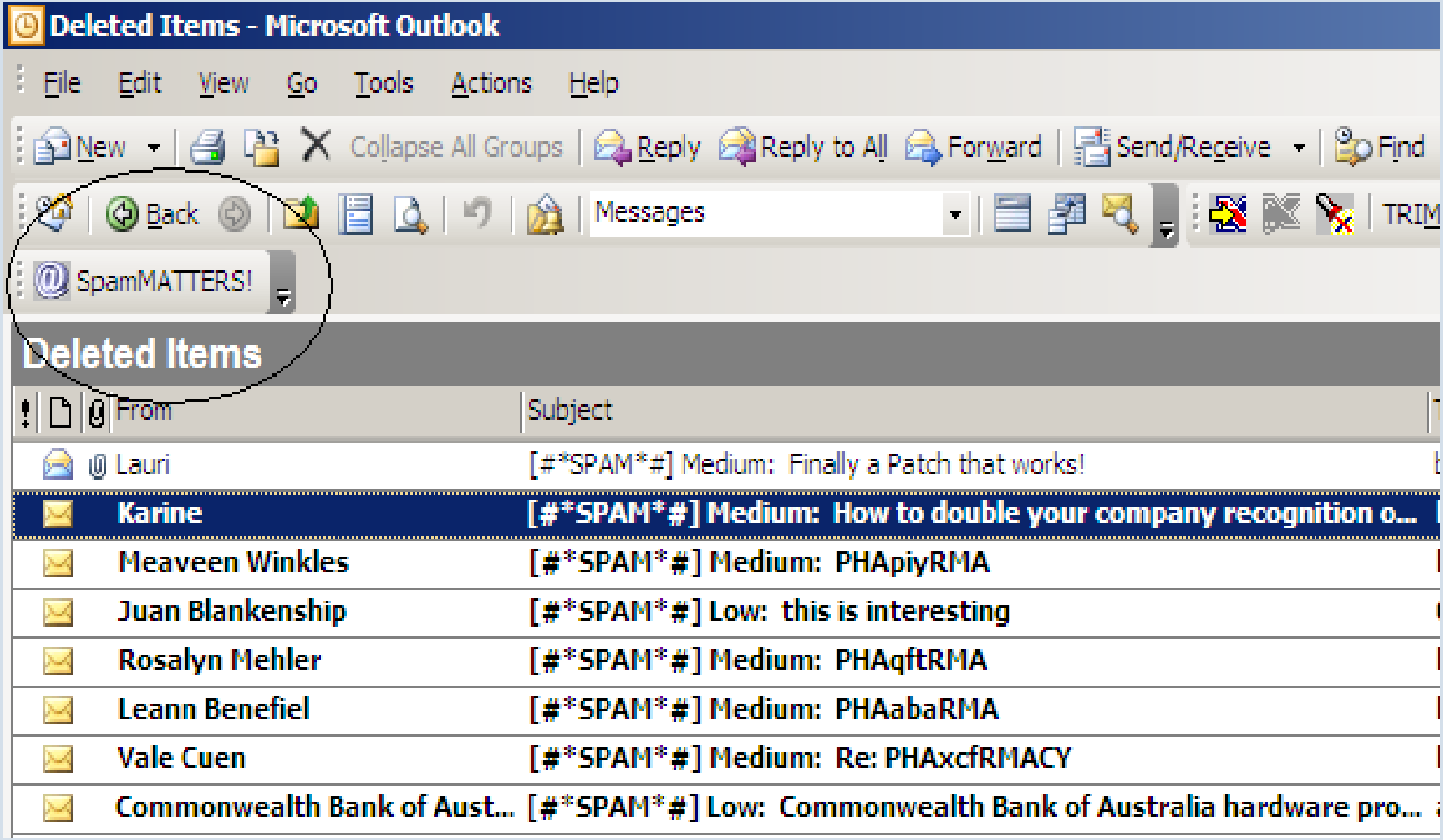
Australian Government
Australian Communications and Media Authority

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/upcoming advances
  - establishment of ISP forum for sharing information on e-security practices and approaches
  - development of portal where ISPs can download AISI data & receive other AISI related information
  - Portal could also contain ‘white list’ of mail servers
  - Provision of reports to organisations other than ISPs
  - Integration of data reported through ACMA’s spam reporting tool – **SpamMATTERS**

Australian Government
Australian Communications and Media Authority

SpamMATTERS – Reporting Button



Australian Government
Australian Communications and Media Authority

AISI relationship to other e-security initiatives

- AISI part of e-Security National Agenda – Securing Australia's Online Environment (ESNA)
- Closely linked to DBCDE initiatives aiming at enhancing the protection of home users and small to medium to enterprises
- Number of 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

your computer
siness safe online
siness self-
ent tool
nsacting online
online
ce
izzes
nd tools
ks
s
ws

This site is designed to help home users and small businesses to stay smart online

Securing your computer

Protect your computer and internet connection from hackers, viruses and theft.

Small business safe online

Information and advice for small businesses to stay sn

Smart transacting online

How to be a smart surfer - shopping and banking safely, and avoiding viruses and scams.

Kids safe online

Protect your children from unsuitable websites and em

Australian Government
Australian Communications and Media Authority

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

Thank you