



Australian Government
**Australian Communications
and Media Authority**

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

www.acma.gov.au

ACMA's technological initiatives in combating spam and enhancing internet e-security

Bruce Matthews
Manager, Anti-Spam Team
Australian Communications & Media Authority

Regional Workshop on Frameworks for Cybersecurity and Critical
Information Infrastructure Protection

Hanoi, Vietnam, 28-31 August 2007



Australian Government

Australian Communications
and Media Authority

Australian Government – Five-Part strategy to combat spam

1. Strong enforcement of the *Spam Act 2003*
2. Education and awareness activities
- 3. Industry measures**
- 4. Technological initiatives and solutions**
5. International cooperation



Legislation – *Spam Act 2003*

- 3 requirements – consent, accurate sender information, and an unsubscribe facility
- ‘Opt-in’ regime, not ‘Opt-out’
- ‘Technology neutral’: email, SMS, MMS, IM
- Complaints growing about spam received on mobiles
- Voice calls not covered, fax currently excluded
- Involves ‘civil penalties’ rather than ‘criminal penalties’
- Increased Australian Government funding in 2007 to combat spam and address e-security issues



Australian Government

Australian Communications
and Media Authority

Spam Act 2003 - Enforcement

- First prosecution under Spam Act in Federal Court – *ACMA v Clarity1/Wayne Mansfield*
- \$5.5m penalties - October 2006
- Found to have sent >200 million emails
- 18 infringement notices (fines)
- \$149,600 penalty recently imposed for mobile spam
- 12 formal warnings
- 6 enforceable undertakings



Australian Government

Australian Communications
and Media Authority

Industry measures to combat spam

- E-Marketing Code of Practice
 - registered by ACMA in March 2005
 - provides guidance to businesses on responsible e-marketing practices
- Internet Industry Spam Code of Practice
 - registered in March 2006
 - specifies measures to reduce the incidence and impact of spam on ISP networks
 - close linkages to e-security



Australian Government

Australian Communications
and Media Authority

ACMA anti-spam enforcement results

- Since April 2004:
 - Australia has dropped from 10th on Sophos list of spamming nations to 28th (for 2006 calendar year)
 - Percentage of global spam originating from Australia has continued to fall – now around 0.5%
 - Only known Australian in top 200 global spammers was successfully prosecuted



Australian Government

Australian Communications
and Media Authority

Technological solutions & monitoring

Two major ACMA initiatives:

SpamMATTERS



Enlisting the support of the public to fight spam

Australian Internet Security Initiative (AISI)

A cooperative arrangement with internet service providers to shut down 'infected' computers



SpamMATTERS technological solution

- SpamMATTERS is a reporting and forensic analysis system ACMA developed to help fight spam
- **Reporting** – Australian email users can report spam to ACMA and delete it with a single click of their mouse
- **Analysis** – SpamMATTERS sorts spam reports into ‘campaigns’, for appropriate action



SpamMATTERS – Reporting Button

The screenshot shows the Microsoft Outlook interface for the 'Deleted Items' folder. The menu bar includes File, Edit, View, Go, Tools, Actions, and Help. The toolbar contains various icons for actions like New, Collapse All Groups, Reply, Reply to All, Forward, Send/Receive, Find, Back, Forward, Messages, and TRIM. A dropdown menu is open, showing an '@' icon and the text 'SpamMATTERS!'. Below this, the 'Deleted Items' folder is displayed as a table with columns for 'From' and 'Subject'. The table lists several spam messages, with the one from 'Karine' highlighted in blue.

From	Subject
@ Lauri	[#*SPAM*#] Medium: Finally a Patch that works!
Karine	[#*SPAM*#] Medium: How to double your company recognition o...
Meaveen Winkles	[#*SPAM*#] Medium: PHApyRMA
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...



Australian Government

Australian Communications
and Media Authority

SpamMATTERS progress to date

- Launched 31 May 2006
- Available for download from ACMA website
- 222,000 registered submitters
- 28 million spam emails reported
- Captures spam bypassing anti-spam filters
- Used to enforce Spam Act and assist national and international authorities
- Strongly supported by ISPs



Australian Government

Australian Communications
and Media Authority

SpamMATTERS data is used to...

- investigate activities of Australian spammers
- ‘criminal’ spam (eg. phishing) is referred to the Australian High Tech Crime Centre
- 800 separate campaigns reported to AHTCC
- shut websites down
- develop reports for overseas authorities on spam originating from their jurisdiction
- China has used these to shut down significant sources of spam



Australian Government

Australian Communications
and Media Authority

SpamMATTERS – future development

- Developed under subcontract by Threatmetrix
- www.spammatters.com
- ACMA has licence to distribute plug-in in Australia
- Although developed for enforcement of Spam Act, looking at other ways data might be used
- Also will integrate with Australian Internet Security Initiative



Australian Government

Australian Communications
and Media Authority

Australian internet security initiative (AISI)

- Trial commenced with 6 ISPs - Nov 2005
- Extended to 25 Australian ISPs - October 2006
- Collects information on compromised computers
- Compares IP address of compromised computer to a list of IP address ranges of Australian ISPs
- Advises relevant ISP of the IP address
- ISP inform customer and liaise with customer to fix
- Customers unaware of compromise
- \$4.7m funding for expansion of AISI in 2007 budget



Example of daily AISI email report

[2007-06-18] - ISI report mailing for XXXXXXXXXX - 259 host(s) detected - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

TRIM

Reply Reply to All Forward

From: Internet Security Initiative [isi@isi.acma.gov.au] Sent: Mon 18/06/2007 11:11 PM

To: [REDACTED]

Cc:

Subject: [2007-06-18] - ISI report mailing for XXXXXXXXXX - 259 host(s) detected

Dear XXXXXXXXXX,

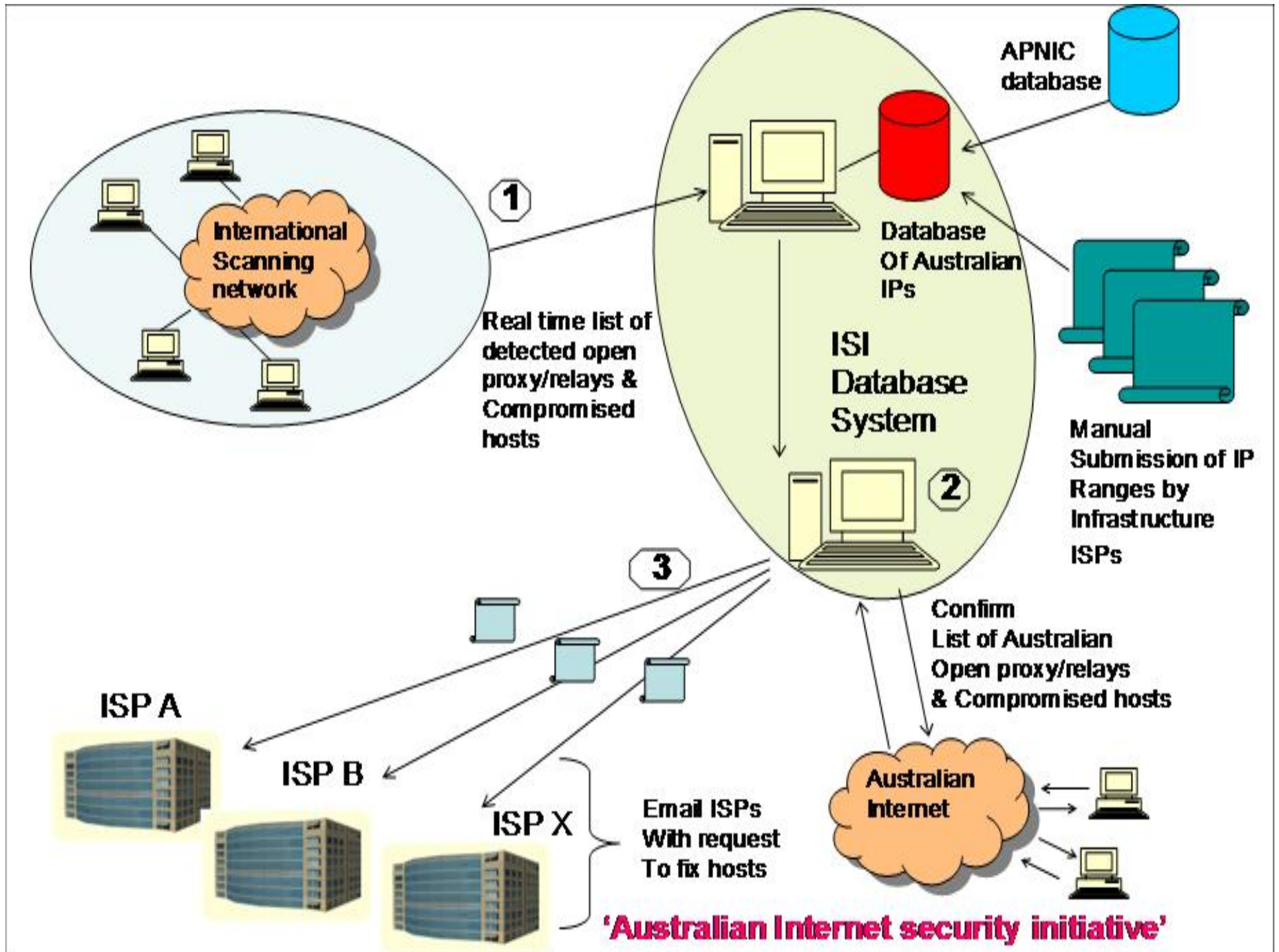
This report is generated by the Australian Communications and Media Authority's Australian Internet Security Initiative (AISI) service.

Below is today's list of open, compromised and zombied hosts on your networks. For help parsing this report, please contact <isi@isi.acma.gov.au>.

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

--- Report follows ---

IPv4 address	Port	Timestamp	Type	Network
58.161. .227	0	2007-06-16 00:27:58	Trojaned:	zombie
58.16. .120.3	0	2007-06-16 01:08:32	Trojaned:	zombie
144.13. .71.12.	0	2007-06-16 06:49:23	Trojaned:	zombie
58.1 1.112.12:	0	2007-06-16 07:46:31	Trojaned:	zombie
58.1 1.11. .24:	0	2007-06-16 08:01:33	Trojaned:	zombie
58.1 1.11 .1.3	0	2007-06-16 08:01:33	Trojaned:	zombie
58.1 1.106.5:	0	2007-06-16 08:06:34	Trojaned:	zombie
58.1 1.6 .7	0	2007-06-16 08:24:35	Trojaned:	zombie
58.17 .5 .7:	0	2007-06-16 09:02:58	Trojaned:	zombie
58.1 1.1. .0.8	0	2007-06-16 09:19:00	Trojaned:	zombie
58.1 1.12 .32	0	2007-06-16 09:30:32	Trojaned:	zombie
58.1 1.11 .5:	0	2007-06-16 09:30:32	Trojaned:	zombie
58.1 1.1 .5. .2	0	2007-06-16 09:36:34	Trojaned:	zombie
58.1 1. 9.2 .7	0	2007-06-16 09:38:35	Trojaned:	zombie
58.1 1. 0.1.4	0	2007-06-16 09:48:06	Trojaned:	zombie





Australian Government

Australian Communications
and Media Authority

What will expansion of AISI involve?

- Expansion to significantly more ISPs
- Increasing sources of information feeding into AISI
- Updating of AISI software
- More detailed compromise reports to ISPs
- Assist in education of consumers about steps they can take to prevent compromises
- Working with ISPs to examine information provided to customers with a compromise
- Working internationally to fight botnets – assisting ITU project



Australian Government
**Australian Communications
and Media Authority**

Thank you

For more information, please go to:

www.spam.acma.gov.au