



**Australian Government**  
**Australian Communications  
and Media Authority**

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

[www.acma.gov.au](http://www.acma.gov.au)

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

Bruce Matthews  
Manager, Anti-Spam Team

ATUG 2007 'Take Away' SME Breakfast  
Sydney

Friday 15 June 2007



# 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



## *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 over 200 million emails
- ACMA successful on both counts:
  - sending emails without consent, and
  - use of address harvested lists



## ACMA anti-spam enforcement results

- Since the enforcement provisions of the *Spam Act* commenced in April 2004:
  - Australia has dropped from 10<sup>th</sup> on Sophos list of spamming nations to 28<sup>th</sup> (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 with a single click
- **Analysis** – SpamMATTERS sorts spam reports into ‘campaigns’



# 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 ribbon contains various actions like New, Collapse All Groups, Reply, Reply to All, Forward, Send/Receive, and Find. A 'SpamMATTERS!' button is highlighted with a red circle. Below the ribbon, the 'Deleted Items' folder is open, displaying a list of deleted emails. The list has columns for 'From' and 'Subject'. The selected email is from 'Karine' with the subject '[#\*SPAM\*#] Medium: How to double your company recognition o...'. Other emails in the list include messages from Meaveen Winkles, Juan Blankenship, Rosalyn Mehler, Leann Benefiel, Vale Cuen, and Commonwealth Bank of Australia.

From	Subject
@ Lauri	[#*SPAM*#] Medium: Finally a Patch that works!
<b>Karine</b>	<b>[#*SPAM*#] Medium: How to double your company recognition o...</b>
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...



## SpamMATTERS progress to date

- Launched 31 May 2006
- Available from ACMA website
- 207,000 submitters
- Over 25 million spam emails reported
- Captures spam bypassing anti-spam filters
- Used to enforce Spam Act and assist national and international authorities



## SpamMATTERS data is used to...

- Investigate activities of Australian spammers
- ‘Criminal’ spam (eg. ‘phishing’) is referred to the Australian High Tech Crime Centre
- 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



## Recent world wide spam trends

- Around 90 per cent of emails are spam
- Significant rise in image spam – more difficult to detect by anti-spam filters
- Fewer viruses in spam, but more links to websites containing malicious content
- Growth of ‘botnets’ - networks of compromised (zombie) computers controlled remotely
- Botnets now generate 80 to 90 per cent of email spam
- Increasing recognition of botnet problem



## 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 recent budget



# Example of daily AISI email report

[2007-04-20] - ISI report mailing for [REDACTED] - 44 host(s) detected - Message (Plain Text)

From: Internet Security Initiative [isi@isi.acma.gov.au] Sent: Fri 20/04/2007 11:11 PM  
To: isi[REDACTED]@sys-ex-1.sys.local  
Cc:  
Subject: [2007-04-20] - ISI report mailing for [REDACTED] 44 host(s) detected

Dear [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 <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
155.143.[REDACTED]	22367	2007-04-19 21:00:19		socks4
155.143.[REDACTED]	37536	2007-04-19 21:00:22		socks4
155.143.[REDACTED]	22367	2007-04-19 21:00:29		socks5
144.138.[REDACTED]	0	2007-04-19 06:44:47		Trojaned:
60.225.[REDACTED]	0	2007-04-19 20:44:35	Trojaned:	Spybot
144.138.[REDACTED]	0	2007-04-19 21:40:53	Trojaned:	Korgo
138.217.[REDACTED]	0	2007-04-19 22:58:42	Trojaned:	Spybot
144.138.[REDACTED]	1221	2007-04-19 12:33:11	Trojaned:	zombie
60.228.[REDACTED]	1221	2007-04-19 14:54:28	Trojaned:	zombie
203.49.[REDACTED]	1221	2007-04-19 18:01:05	Trojaned:	zombie
203.40.[REDACTED]	1221	2007-04-19 18:10:39	Trojaned:	zombie



**Australian Government**  
**Australian Communications  
and Media Authority**

# Thank you

For more information, please go to:

[www.spam.acma.gov.au](http://www.spam.acma.gov.au)