

COUNTRY UPDATES -

MALAYSIA'S INITIATIVE IN MITIGATING SPAM

ZAHRI YUNOS *ABCP*
Chief Operating Officer
CyberSecurity Malaysia

CSNA-LAP WORKSHOP
Lisbon, Portugal
7-9 Oct 2009



Securing Our Cyberspace



CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656



- **An agency under the Ministry of Science, Technology and Innovation of Malaysia**
- **Started operation in year 1997 and funded by the Malaysian Government**
- **We host the Malaysian Computer Emergency Response Team (MyCERT), the national CERT**

CYBERSECURITY MALAYSIA SERVICES



MyCERT
CYBER999
REPORTING
INCIDENTS &
ALERTS

Digital Forensics
Find... Ctrl+
Find Next 3
Cyber Forensics Investigations
CYBER CSI

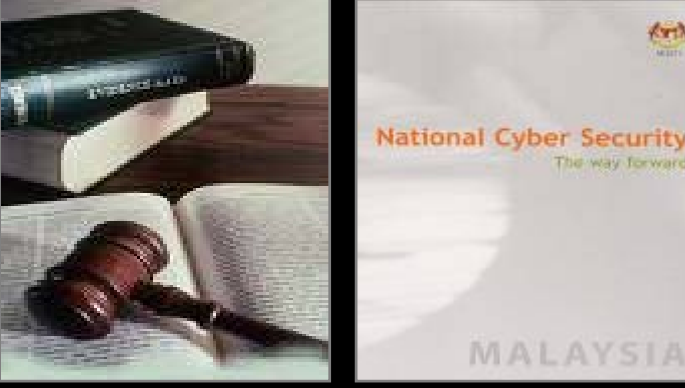
Cyber Security Emergency Services



Security Management & Best Practises
ISO/IEC 18043:2006
ISO/IEC 18028-1:2006
ISO/IEC 17799:2005
ISO/IEC 18028-2:2006
ISO/IEC 18028-3:2005
ISO/IEC 18028-4:2005
ISO/IEC 18028-5:2006
ISO/IEC TR 18044:2004
ISO/IEC 27001:2005

Security Assurance

Security Quality Management Services



National Cyber Security
The way forward
MALAYSIA

Strategic Policy & Cyber Media Research



eSecurity
TOWARDS BUILDING A SECURITY CULTURE

Training & Outreach

INTRODUCTION – DEFINITION OF SPAM BY MALAYSIA

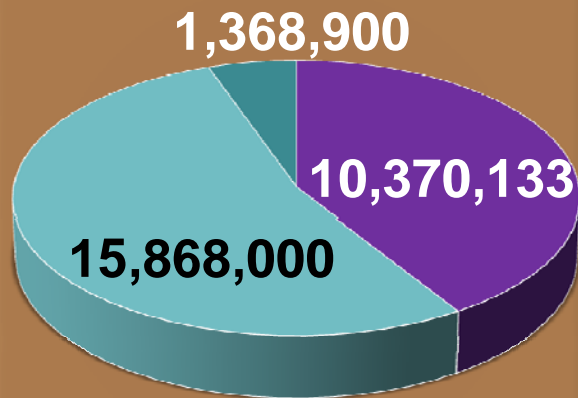
“**Unsolicited electronic messages** sent through various communication modes including but not limited to e-mails, mobile short message service (SMS) or instant messaging services where there is **no prior relationship** between the sender and the recipient regardless of content whether **commercial or non-commercial** messages including malicious program and/or data”

*- Anti-Spam Toolkit, Malaysian Communications
and Multimedia Commission 2006*

ICT AND INTERNET GROWTH IN MALAYSIA

DEMOGRAPHIC

Internet Users in Malaysia
June 2008



- Non-Internet Users
- Internet Users
- Broadband Users

ICT INDUSTRY IS A GROWING



Malaysia ICT sector to see 4%-5% growth:
 - 2009 is expected to see a growth in local ICT industry despite the global economic slowdown

ICT DEVELOPMENT OPPORTUNITY

- increasing broadband penetration to 50% by 2010
- tax incentives for employers who buy new PCs and pay for their employees' broadband connections

Malaysian IT spending total USD\$4.3 billion in 2008
 Source: Business Monitor International (May 2009)

Worldwide security software market revenue totalled \$13.5 billion in 2008
 Source: Gartner (June 2009)

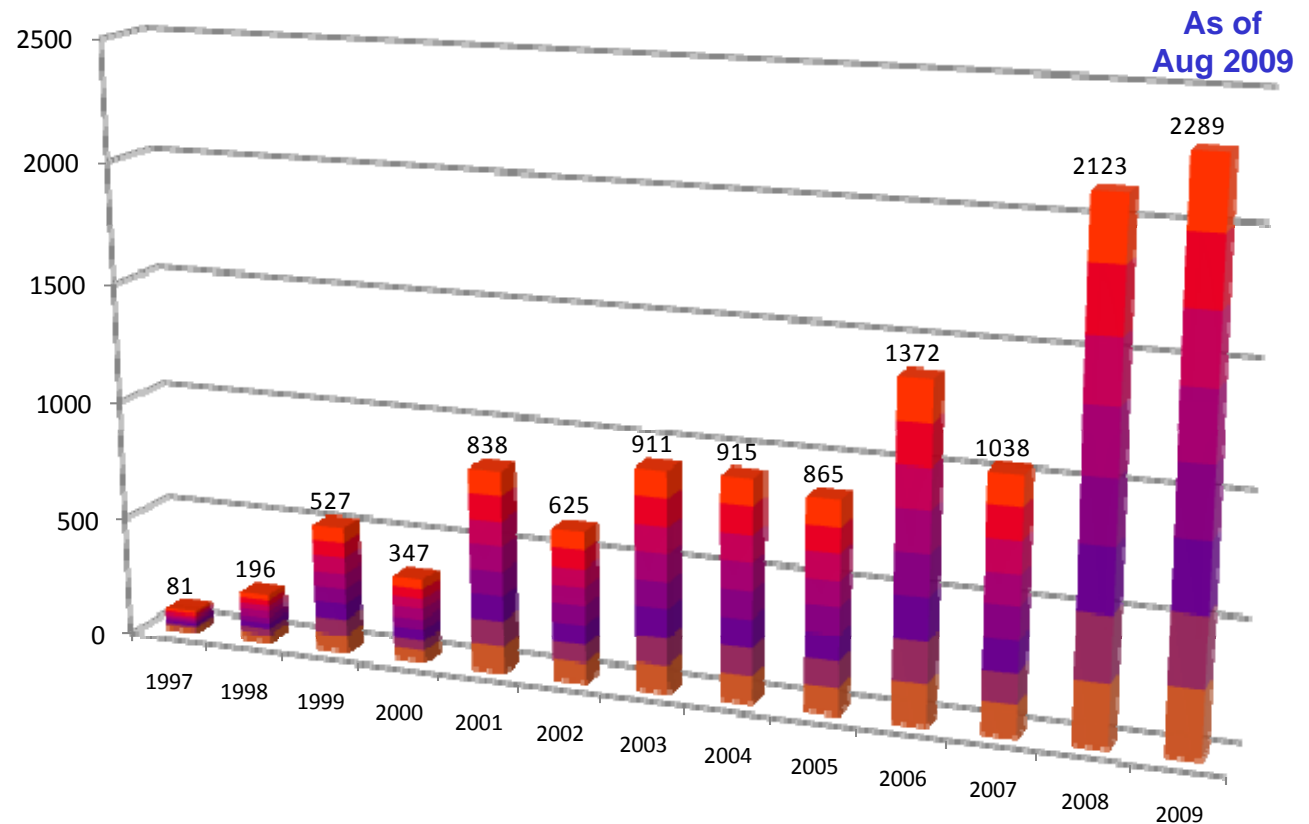
Worldwide IT spending total USD\$3.4 trillion in 2008
 Source: Gartner (June 2009)

CYBER SECURITY INCIDENTS (1997-2009)

- A total of 12,127 security incidents were referred since 1997 (excluding spam)

Type of incidents:

- Intrusion
- Destruction
- Denial-of-Service
- Virus
- Hack Threat
- Forgery
- Harassment



SPAM STATISTICS 2009

– DATA GATHERED BY CYBERSECURITY MALAYSIA

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Spam rejected during connection	5334	6272	4814	3619	4157	3865	26293	18199	-	-	-	-	72553
Spam filtered by filtering devices	4169	4796	4118	4800	5645	5223	7446	4740	-	-	-	-	40937
TOTAL	9503	11068	8932	8419	9802	9088	33739	22939	-	-	-	-	113490

❑ Spam rejected during connection:

- *Rejection of IPs and known subnets containing spam that attempted to establish connection*

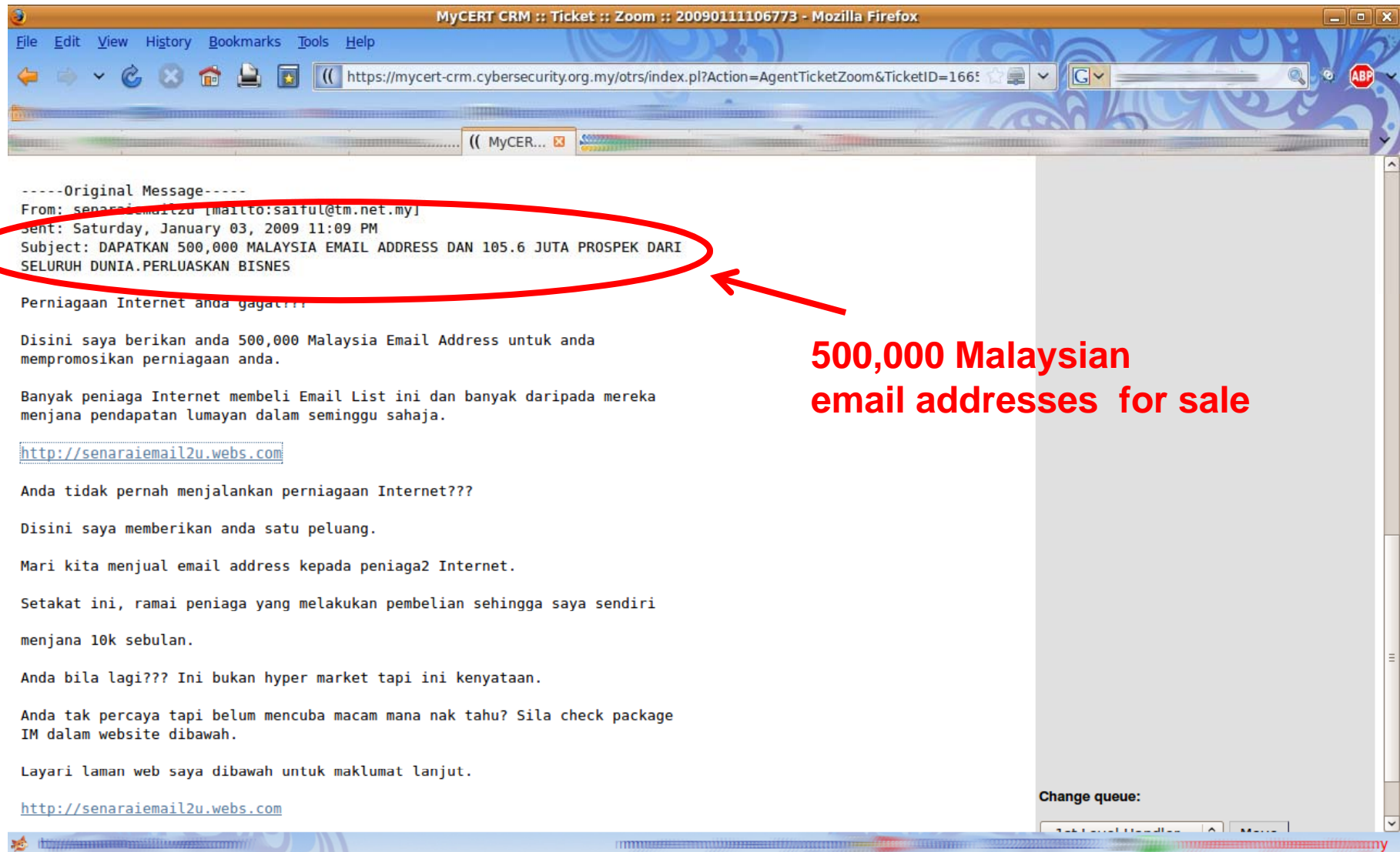
❑ Spam filtered by filtering devices: Types of contents

- *Virus*
- *Phishing*
- *Unsolicited message such adult content, business, political message, lottery winner, scam awards, etc*

* *Spike in July was due to software upgrading: resulted more detection and better filtering*



CASE STUDY - SPAM BUSINESS



**500,000 Malaysian
email addresses for sale**

CASE STUDY - SPAM CONTAINING PHISHING

Subject:
CONTACT US IMMEDIATELY
From:
"<snipped>" <active@quicknem5.com>
Date:
Tue, 15 Sep 2009 19:33:04 -0700
To:

Dear Valued Customer,

Due to the increasing spam attack on our customers, we have introduced an advanced protection to protect all M2U users. You are hereby required to immediately protect your account below as unprotected accounts will be terminated till further notice.

SECURE YOUR ACCOUNT NOW
newxprotectionm2u.com/M2ULogin.htm

Sincerely,

<snipped> Group

	Q1 09	Q2 09	TOTAL
Local Bank	68	48	116
Others	45	43	88
TOTAL	113	91	204

CASE STUDY - GET RICH SCHEME

Subject: [MyCERT-200907091025662] JANGAN BUKA EMAIL INI JIKA ANDA SUDAH KAYA!
 Date: Thu, 9 Jul 2009 14:30:05 +0800
 From: OTRS Notification Master <otrs@mycert-crm.cybersecurity.org.my>
 Organization: CyberSecurity Malaysia
 To: <snipped>@cybersecurity.org.my

Pemegang Kad Kredit Berjaya <rahsiakadkredit@gmail.com> wrote:



Testimoni

Apa kata pelanggan yang telah mencubanya?

Tetapi kalau anda ingin buat duit cepat dan mudah di internet sila hyperlink dibawah:

<http://k.my/kadkredit>

RM17,200 Dengan Teknik Anda Setakat Ini!

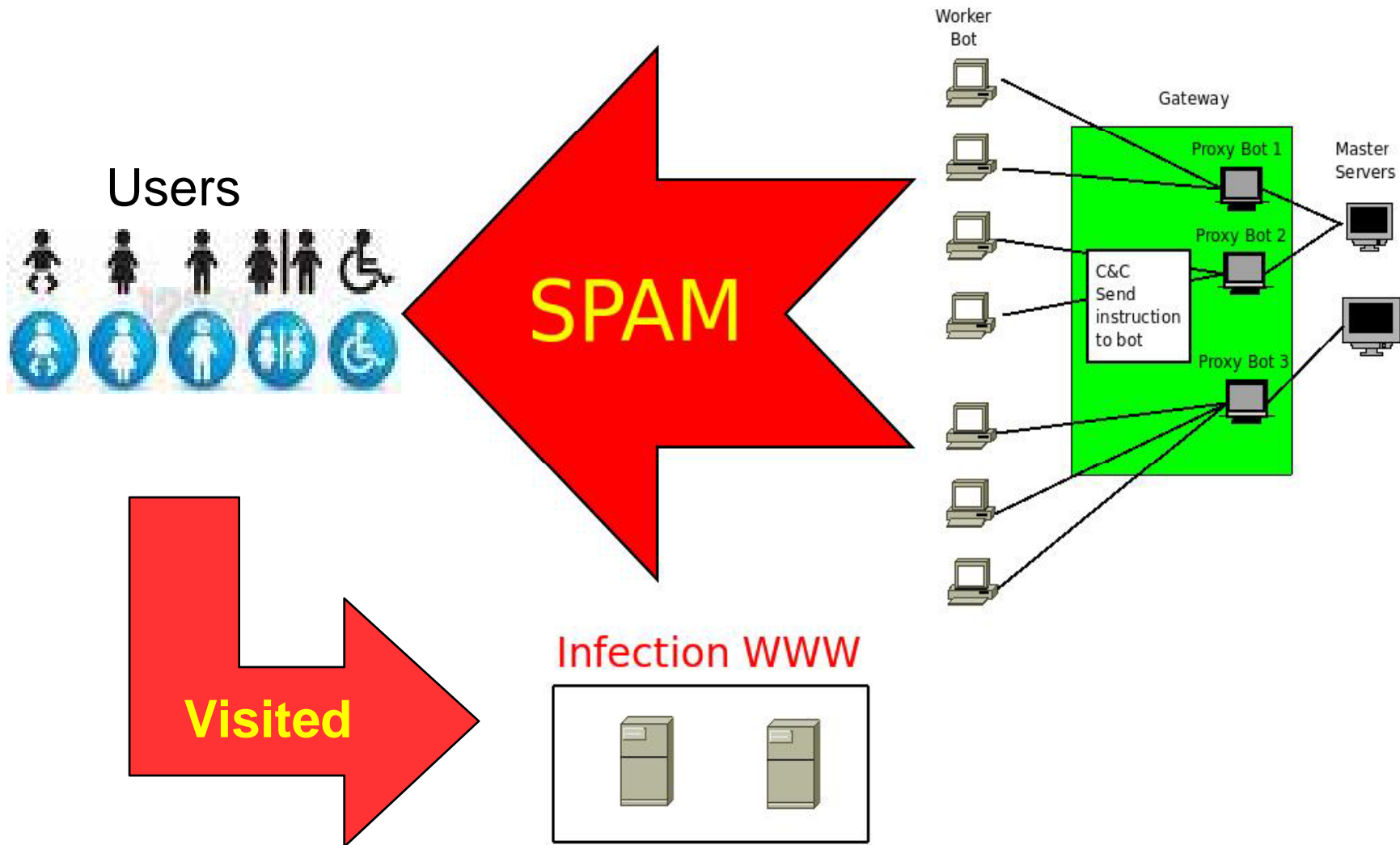
" Apa rahsia anda sehingga hari minggu pun saya boleh dapat komisen, sehingga meledak **RM1300** sehari!! Macam nak pengsan rasanya apabila saya menerima email dari maybank2u beritahu ada RM150, RM450 masuk ke akaun saya hampir **SETIAP HARI!** Kini saya menjana lebih RM17,200 dengan sistem anda. Nizam, tak sia-sia saya ikut saudara selama ni!"

Type : Wadiah Savings Account Account No : 164137434057
 Balance : RM2,818.58 Available Balance : RM2,818.58

Transaction History			
Transaction Date	Description	Debit	Credit
17-Nov-2007	FUND TRANSFER TO A/C		RM700.00
17-Nov-2007	TRANSFER FROM A/C	RM100.00	
16-Nov-2007	TRANSFER FROM A/C	RM350.00	
15-Nov-2007	DEBIT ADVICE	RM100.00	
15-Nov-2007	DEBIT ADVISE	RM100.00	
14-Nov-2007	FUND TRANSFER TO A/C		RM100.00
13-Nov-2007	FUND TRANSFER TO A/C		RM100.00
12-Nov-2007	FUND TRANSFER TO A/C		RM100.00
11-Nov-2007	FUND TRANSFER TO A/C		RM200.00
10-Nov-2007	CASH WITHDRAWAL	RM500.00	
10-Nov-2007	CASH WITHDRAWAL	RM1,500.00	
09-Nov-2007	FUND TRANSFER TO A/C		RM400.00
08-Nov-2007	CASH DEPOSIT		RM1,200.00
08-Nov-2007	FUND TRANSFER TO A/C		RM900.00
06-Nov-2007	CASH WITHDRAWAL	RM1,001.00	

Komisen dari FLB PRO = RM2,500
 (Data tempoh 10 HARI)

HOW SPAM IS CRAFTED



PROJECTHONEYPORT – HARVESTER IP

Directory of Harvester IPs

This page displays the top IPs by different categories. You may sort or limit this list by selecting from the menus below.

Global Statistics

Total Bad Events

Harvesters

From All Countries

See [comment spammers](#), [dictionary attackers](#), or [mail servers](#) from the same region.

You may also [lookup information](#) on a specific IP address.

To track IPs targeting a website not currently listed in the pulldown, simply [install a honey pot](#) on it.

An [RSS feed](#) for this page is available.

The list below is comprised of Harvester IPs (limited to the top 50) that are:

- Arranged by their **Total Bad Events**

Harvester IP	Event	Total	First	Last
200.226.134.53 HC	Bad Event	150,163	2007-10-19	2007-12-07
93.174.93.220 HC	Bad Event	108,551	2008-07-25	2008-09-16
64.27.5.162 HC	Bad Event	100,779	2007-03-06	2008-08-14
93.189.56.218 HC	Bad Event	100,364	2008-07-24	2008-08-14
64.233.166.136 Se	Bad Event	72,159	2005-04-21	2008-08-08
195.229.242.154 HC	Bad Event	64,720	2008-01-23	2008-03-31
64.233.178.136 Se	Bad Event	58,546	2005-04-21	2008-11-16
66.249.90.136 Se	Bad Event	51,187	2006-12-27	2009-02-27
203.144.144.164 HC	Bad Event	44,111	2006-03-22	2008-07-04
72.14.220.136 Se	Bad Event	39,470	2006-11-23	2009-01-14
200.65.127.161 HC	Bad Event	36,445	2007-10-24	2009-09-07
165.228.133.11 HC	Bad Event	36,114	2006-07-30	2008-04-09
193.53.87.77 HC	Bad Event	31,349	2008-07-02	2008-08-05
200.61.176.77 HS	Bad Event	30,885	2007-06-27	2009-03-09
165.228.130.12 HC	Bad Event	30,695	2005-06-01	2008-04-09
62.163.80.205 H	Bad Event	29,332	2007-02-06	2007-09-12
208.223.208.181 H	Bad Event	27,911	2005-02-03	2008-08-14
209.85.138.136 Se	Bad Event	27,065	2007-03-27	2008-12-30
64.34.255.239 HC	Bad Event	24,461	2007-08-18	2008-12-12
72.14.252.136 Se	Bad Event	23,974	2006-11-19	2008-08-14
210.19.199.146 HSD	Bad Event	22,992	2007-10-16	2009-09-05
210.239.30.136 HC	Bad Event	22,919	2007-07-10	2008-07-10
165.228.131.12 HC	Bad Event	22,625	2005-05-10	2008-04-10
219.93.178.162 HC	Bad Event	21,569	2007-04-29	2009-08-05



TOP SPAM SERVER IP

Directory of Spam Server IPs

This page displays the top IPs by different categories. You may sort or limit this list by selecting from the menus below.

Global Statistics
 Total Spams (E-mail)
 Spam Servers
 Malaysia
 From Any Region

See [comment spammers](#), [dictionary attackers](#), or [mail servers](#) from the same region.






















You may also [lookup information](#) on a specific IP address.

To track IPs targeting a website not currently listed in the pulldown, simply [install a honey pot](#) on it.

An [RSS feed](#) for this page is available.

The list below is comprised of Spam Server IPs (limited to the top 50) that are:

- Arranged by their **Total Spams (E-mail)**
- Located in the **Malaysia**

Spam Server IP	Event	Total	First	Last
 203.82.79.101 SDC	Spam	9,669	2009-04-20	2009-09-07
 203.82.79.104 SD	Spam	9,295	2009-04-20	2009-09-07
 203.82.91.102 HSD	Spam	9,078	2009-04-20	2009-09-07
 203.82.79.102 SD	Spam	9,046	2009-04-20	2009-09-07
 203.82.91.104 SD	Spam	8,852	2009-04-20	2009-09-07
 203.82.79.103 SD	Spam	8,669	2009-04-20	2009-09-07
 203.82.91.101 HSD	Spam	8,668	2009-04-20	2009-09-07
 203.82.79.2 SD	Spam	8,532	2008-12-17	2009-04-20
 203.82.91.34 HSD	Spam	8,312	2009-01-13	2009-04-20
 218.111.120.149 SD	Spam	6,961	2006-08-02	2009-09-07
 203.223.151.54 S	Spam	6,155	2006-07-05	2006-08-02
 123.136.101.197 SDC	Spam	5,510	2008-03-07	2009-09-07
 210.19.199.146 HSD	Spam	4,923	2007-10-16	2009-09-05
 61.4.104.38 SD	Spam	4,674	2009-05-30	2009-08-13
 60.54.191.10 SD	Spam	4,394	2008-09-05	2009-09-07
 60.49.230.214 SD	Spam	4,278	2008-03-08	2009-09-07
 124.82.154.102 SD	Spam	4,168	2008-08-15	2009-09-07
 60.54.191.34 SD	Spam	4,103	2008-03-08	2009-09-07
 61.6.56.23 SD	Spam	3,959	2007-07-17	2009-09-03
 219.94.6.142 SD	Spam	3,735	2008-10-17	2009-09-07
 202.60.56.221 SD	Spam	3,619	2008-11-16	2009-09-07

REPORTING SPAM INCIDENT

From: Malaysia Computer Emergency Response Team <mycert@mycert.org.my>
To: abuse@<snipped>
Subject:
Re: [MyCERT-200907221028525] Reporting an Incident: Spam Email
Created: 07/22/2009 17:04:09
Dear Abuse Team,

MyCERT received a report from a local organization regarding spam email originating from an IP address under your administration:

IP address: 203.82.79.101

Attached is the full header of the spam email and whois for your analysis purpose. Please check your user's traffic and take appropriate action against him/her in order to put a stop to such activities.

Appreciate your prompt action.

For correspondence regarding the above issue, please retain the above subject header: [MyCERT-200907221028525] to ensure effective response.

Regards,
-<snipped>



CURRENT SITUATION

- ❑ Malaysia in the top 40 lists of world spam harvester activities (source projecthoneypot.org)
- ❑ No specific anti-spam law yet – in the midst of review by Government
- ❑ Anti-spam measures in Malaysia
 - Self regulation approach (through education and creation of awareness and technology solutions), management of service providers and international collaboration
 - *Borderware Security Appliance - linked with reputable lists of spam blacklists and provide Defense-In-Depth for Virus, Spam and Malware Prevention*

COMMUNICATIONS AND MULTIMEDIA ACT 1998 AGAINST SPAMMERS

- ❑ Malaysia's Communications and Multimedia Act 1998 under Section 233(1) is applied against spammers



- ❑ Section 233. Improper use of network facilities or network service, etc.

(1) A person who

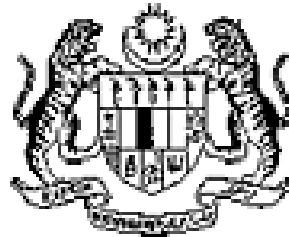
(a) by means of any network facilities or network and service or applications service knowingly

(b) makes, creates or solicits; and

(c) initiates the transmission of,

Any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person

PENALTY UNDER THIS SECTION



LAWS OF MALAYSIA

Act 588

Communications and Multimedia Act 1998

A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding RM50,000 (Fifty Thousand Ringgit) or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 (One Thousand Ringgit) for every day during which the offence is continued after conviction.

INTERNET BANKING TASK FORCE (IBTF)

- Set up in 2004
- Platform for sharing recent Internet banking fraud cases and where appropriate, propose responses and solutions.
- Members include local commercial banks, regulators bodies, enforcement authorities, ISP and CyberSecurity Malaysia
- Formulate Incident Response Plan and establish standardized reporting procedures
- Collaborate with other agencies or authorities in handling phishing and information security incidents faced by banks



ISSUES AND CHALLENGES

- ❑ Spam in Russian and Malay characters that make them difficult to be detected by spamfilter
- ❑ CAPTCHA - Breaking tools to compromise CAPTCHA becoming sophisticated
- ❑ The problem of mitigating botnet inherited in spam - IP involves spamming is increasing
- ❑ Absence of/differences in anti-spam laws between countries make anti-spam efforts difficult
- ❑ Some spam involve promoting legal businesses and might be acceptable to some users

CONCLUSION

- ❑ Spam is a growing problem and it causes nuisance - anti-spam efforts requires a global co-operation
- ❑ Education and awareness, compliance and enforcement, and placing proper technologies are fundamentals in handling spam
- ❑ Best practices and technical guidelines to fight spam and to minimise spam incidents
- ❑ Anti-spam laws/regulations is to be harmonised globally

THANK YOU

Websites

CyberSecurity
MALAYSIA
www.cybersecurity.my

CNII Portal
Critical National Information Infrastructure
cnii.cybersecurity.my

CYBER999
REPORTING
INCIDENTS &
ALERTS
MyCERT
Malaysian
Computer
Emergency
Response
Team

www.mycert.org.my

eSecurity

TOWARDS BUILDING A SECURITY CULTURE
TO MYDCR BUILDING A SECURITY CULTURE

www.esecurity.org.my

Emails



for general
inquiries

info@cybersecurity.my



for incidence
reporting

cyber999@cybersecurity.my

