A week in the life of security@apnic.net (IRT email address)

Frank Salanitri

Project & Systems Services Manager, APNIC

What is APNIC role in preventing network abuse?

- As a registry, APNIC **adopts and applies policies** for it's community which address network abuse. APNIC does not have the capacity to investigate abuse complaints or the legal powers to regulate Internet activity.

- APNIC seeks to raise awareness of the need for **responsible network management in the Asia Pacific**, through training and communication.

How to address abuse complaints

- If a search refers you to APNIC, it means that the network in question is registered in the Asia Pacific region.
- Use APNIC Whois Database to get contact information on the network involved.
- If you are not able to get the cooperation of the network administrators, then you need to contact law enforcement agencies either in your jurisdiction or the jurisdiction where the problem originates.
- http://www.apnic.net/apnic-info/whois_search/abuse-and-spamming/reporting-abuse-and-spam

IRT Object

- Reporting of network abuse can be directed to specialized teams such as Incident Response Teams (IRTs)
- Implemented in AP region by policy Prop-079 in November 2010.
  - Mandatory for inetnum, inet6num and aut-num objects created and updated in whois database.

```
inetnum:        1.0.0.0 - 1.255.255.255
netname:        APNIC-AP
descr:          Asia Pacific Network Information Centre
descr:          Regional Internet Registry for the Asia-Pacific Region
descr:          6 Cordelia Street
descr:          PO Box 3646
descr:          South Brisbane, QLD 4101
descr:          Australia
country:        AU
admin-c:        HM20-AP
tech-c:         NO4-AP
mnt-by:         APNIC-HM
mnt-lower:      APNIC-HM
mnt-irt:        IRT-APNIC-AP
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20100120
changed:        hm-changed@apnic.net 20101116
changed:        hm-changed@apnic.net 20110114
source:         APNIC
```

```
irt:            IRT-APNIC-AP
address:        Brisbane, Australia
e-mail:         helpdesk@apnic.net
abuse-mailbox:  security@apnic.net
admin-c:        HM20-AP
tech-c:         NO4-AP
auth:           MD5-PW $1$4Xs0dCYW$2n3kQaMpxGmUyAcaKYaui/
remarks:        APNIC is a Regional Internet Registry.
remarks:        We do not operate the referring network and
remarks:        is unable to investigate complaints of network abuse.
remarks:        For more information, see www.apnic.net/irt
mnt-by:         APNIC-HM
changed:        hm-changed@apnic.net 20101111
changed:        hm-changed@apnic.net 20110124
source:         APNIC
```

How many complaints?

Abuse Types / Abuse Type	Complaint Date / Month: Feb / 2011	Mar / 2011	Apr / 2011	May / 2011	Jun / 2011	Total
Spam Complaint	4,337	18,917	15,833	4,806	236	44,129
Mail Server Attack	700	1,119	532	358	2,486	5,195
Attack	195	586	635	164	2	1,582
Bruteforce	157	438	330	105	0	1,030
Botnet	47	348	219	78	78	770
Netscan	113	286	159	66	0	624
DDOS	71	181	166	50	1	469
Hacking	94	161	133	41	0	429
Port Scan	43	133	121	57	2	356
Blank	22	0	100	65	29	216
Phishing	8	42	23	15	0	88
Fraudulent site	11	60	15	2	0	88
Spam	1	48	16	9	2	76
Trademark/content	0	17	6	32	8	63
Malware	0	18	25	1	0	44
Total	5,799	22,354	18,313	5,849	2,844	55,159

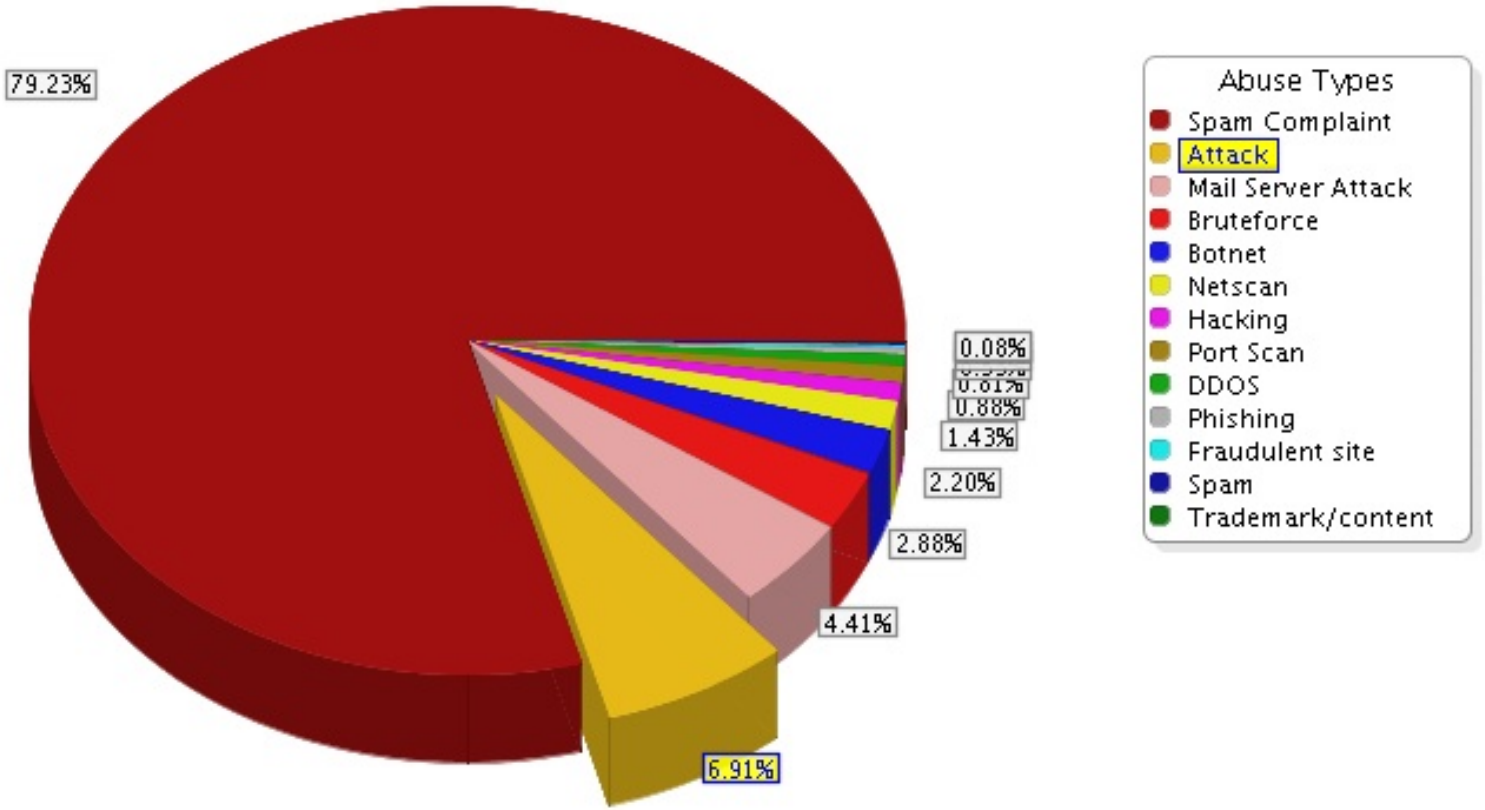
Example abuse complaints

- http://www.dnsbl.de/
  - #1711061: DNSBL: unsolicited email from your network 113.171.104.0
- http://blacklist.woody.ch/
  - Abuse report about 210.125.221.66
- http://www.blocklist.de
  - [noreply] abuse report about 61.183.16.199 - Thu, 24 Mar 2011 11:20:22 +0100 -- service: ssh (Again x 10) RID: 815438
  - [noreply] abuse report about 59.94.243.90 - Thu, 24 Mar 2011 11:31:29 +0100 -- service: mail (First x 1) RID: 815144

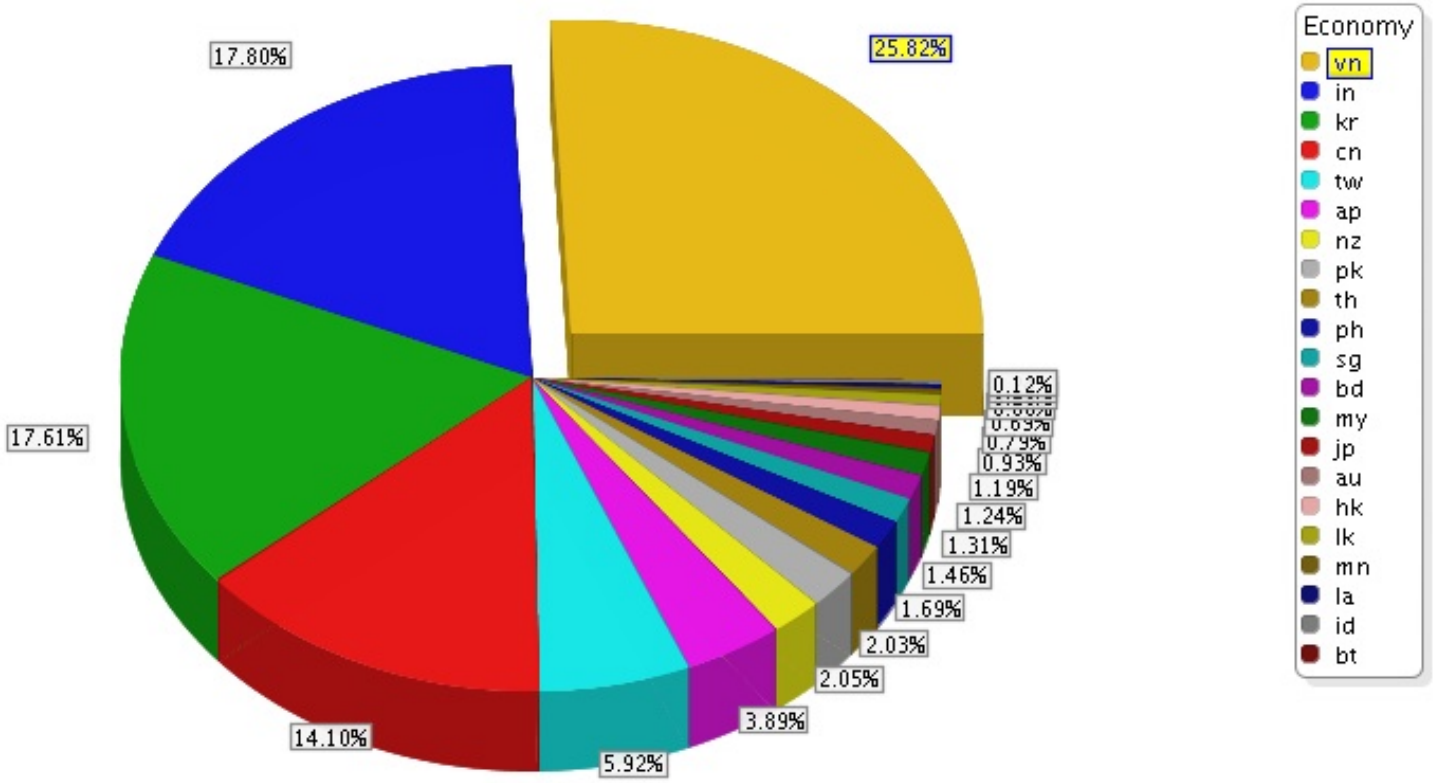
Snapshot 14th – 20th March 2011

Abuse Types	Week					
Abuse Type	Week 1	Week 2	Week 3	Week 4	Week 5	Total
Spam Compl...	5,306	6,560	4,208	2,816	27	18,917
Mail Server A...	291	382	234	181	31	1,119
Attack	78	82	367	59	0	586
Bruteforce	98	97	153	90	0	438
Botnet	50	85	117	96	0	348
Netscan	66	87	76	56	1	286
DDOS	80	23	29	43	6	181
Hacking	44	40	47	30	0	161
Port Scan	27	33	43	30	0	133
Fraudulent site	10	5	9	30	6	60
Spam	4	12	8	13	11	48
Phishing	8	13	16	5	0	42
Malware	3	4	0	11	0	18
Trademark/c...	5	4	4	3	1	17
Total	6,070	7,427	5,311	3,463	83	22,354

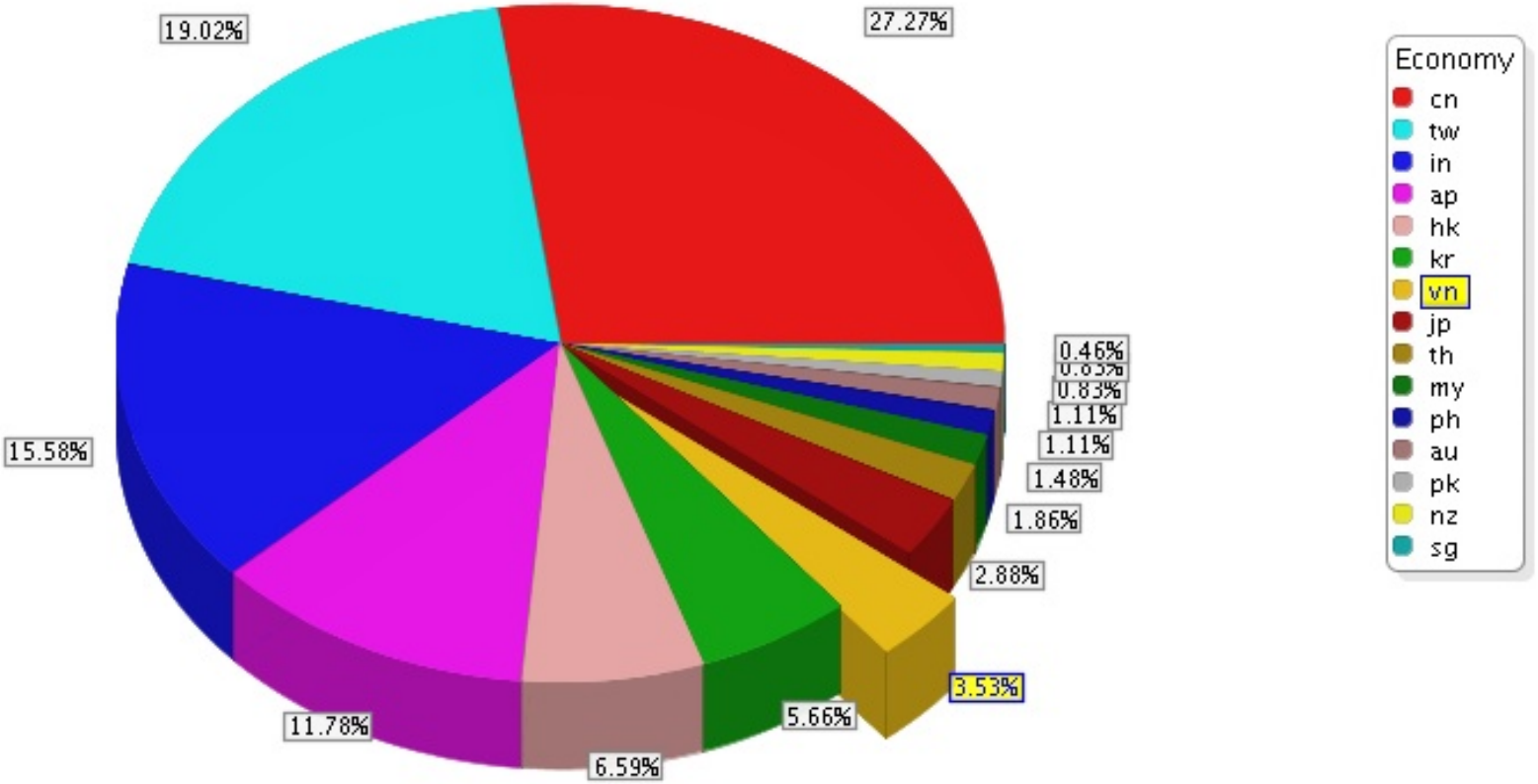
Distribution of Complaints for the week



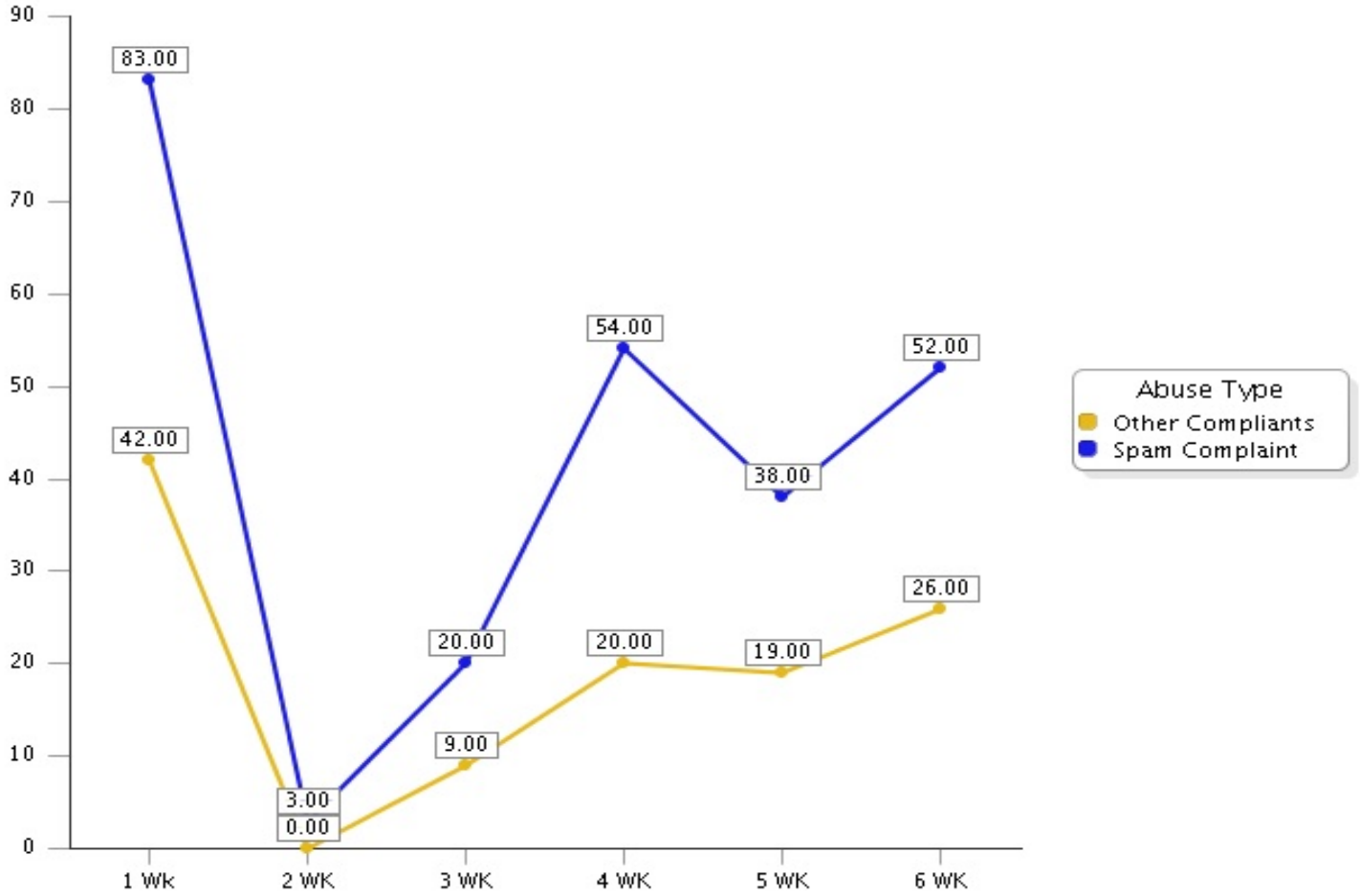
Distribution of email type complains by economy



Distribution of Non-email type complains by economy



Recurring IP Usage over 6 weeks



Blacklisted 5 months later

- Querying DNSBL zen.spamhaus.org

Complaint Type	Distinct IPs	Number blacklisted 5 August 2011	Number blacklisted 11 August 2011
Spam	2591	21 (.8%) spam only	20 spam only
Other	622	48 (8%) exploits, trojans	49) exploits, trojans
All complaints	3213		343

Observations

- Spammers and attackers generally move on.
- However there is a pattern of address reuse.
- IP Addresses do get blacklisted.
- Addresses do remain in blacklists.
- APNIC cannot avoid tainted address returns.
- APNIC tests returned address space but will current tests be sufficient before reuse?

Questions ?