SPAM: 101
Cause and Effect

JARING
come together

Table of Contents

- Background: JARING
- SPAM 101
- Effects
- Lesson Learned
- Challenges and Propositions

JARING
come together

Part I: Background on JARING

(We're the good guys.)

What is JARING?

- The first ISP in Malaysia (1992: 28 subscribers).
- Today: 800,000 subscribers
- Services:-
  - Dial Up, Office Broadband, Wireless Broadband, Dedicated Access, Secure VPN, VOIP
  - Secure Internet Data Centre, Web Hosting, Firewall Solution, E-mail.
- 6 * /16, 2 * /17, 1 * /18 = 475,136 addresses
- 8% is allocated for dynamic IP addresses

Part II: SPAM 101

(A lot of good things, just focusing on one of the not so good ones, with spammers mostly.)

What is Spam and Malware in E-Mail Context?

- Definitions in the context of JARING E-Mail Service:-
- Spam: Unsolicited, bulk mail operations. Examples:-
  - Mails duplicated and sent to a high percentage of users, sometimes in a distributed fashion
  - Dictionary attacks launched to harvest working ISP e-mail addresses
- Malware: Unsolicited mail with virus or worm attached to it.
  - Normally a seasonal phenomena
  - Sizable increase of malware in mails in 2004.

Incoming Spam: Impacts to ISPs

- Waste of Resources: 50-80% of e-mail traffic is Spam.
- Difficulty of Management: E-mail traffic has spikes, i.e. seasonal malware attacks (MyDoom, Bagle, Netsky).
- Performance Impact: performance hit in delivering, fetching and managing mails.
- Inconvenience/Nuisance to customers: A JARING E-mail account receives on average 5-20 spam e-mails per day, depending on popularity of e-mail address in spammers' databases.

JARING
come together

Incoming Spam: How do ISPs get spammed?

- Spammers or malware harvest addresses by collecting published / semi-published information using multiple harvesting techniques:-
  - Collect e-mail addresses from websites
  - Collect e-mail addresses from newsgroups
  - Collect e-mail addresses from mailing list archives
  - Fake mails to ISPs to collect probably active e-mail addresses (dictionary attacks).
- Spam gets sent from:-
  - Spammer-friendly networks (i.e. networks in blocklists)
  - Compromised systems by crackers or malware (increasing!)

JARING
come together

Outgoing/Linked Spam:
How do ISP networks get enlisted into SPAM and Anti SPAMMER's database

- Hosts machines vulnerable to intrusions and exploits by crackers and/or spammers:-
  - Open Relay/Proxy: mis-configured / worm-infected host which allows anyone, anywhere to send mail to any address in the Internet.
    - Mis-configured open relays/proxies: often occur in leased line customers who run their own mail or proxy servers.
    - Worm-infected open relays: often occur in individual dial-up or broadband users, i.e. dynamic IP range.

JARING come together

Part III: Effects

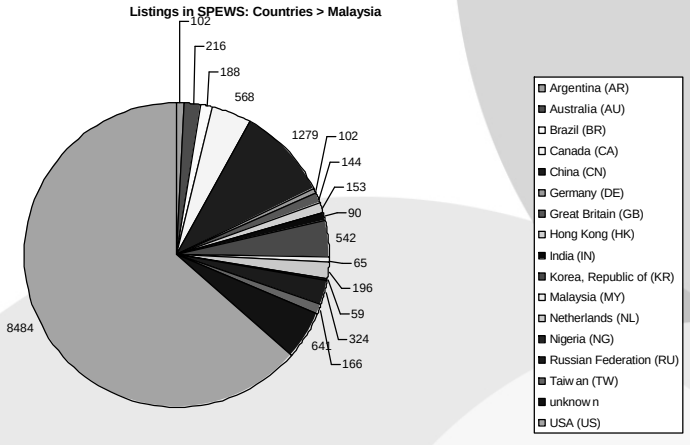
JARING come together

Enlistment into Anti-SPAMMER's database

- "Spamvertizing". Example: JARING's past SPEWS entry:-
  - SPEWS evidence S2062: the 2 parties:-
    - PERPAY-TWO (PerPay.com / PerPay Sdn Bhd):-
      - JARING delegated 61.6.67.88 – 61.6.67.95 range
      - Range used to host DNS records for Bullet9 (ns1.exubient.com),
      - Range used to host web space for spammer, i.e. "spamvertizing": http://www.wwecourse.com/…:-
      - The URL is linked to in spam mails.
      - Basically hosts more information / supporting system fpr the products and services being advertised by spammers.
    - Bullet9 (Bullet9 Communications):-
      - Major spammer web hosting and bulk mail advertiser, with resources in Malaysia and Russia).

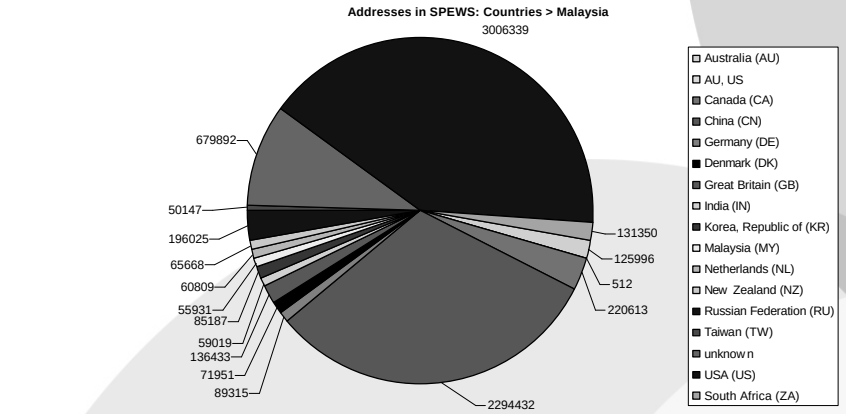
JARING come together

July 2003: Listing in Popular Blocklists (Countries)



JARING come together

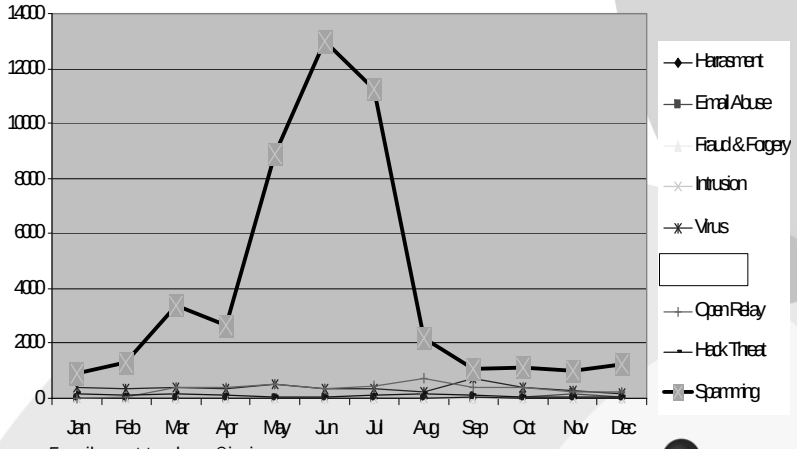
July 2003: Addresses in Popular Blocklists (Countries)



Total Addresses in SPEWS: 7347714

JARING come together

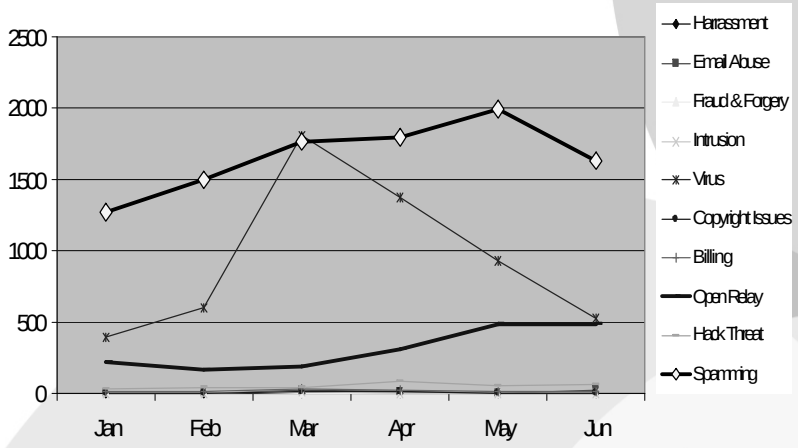
JARING Incident Reports (2003)



Source : Emails sent to abuse@jaring.my

JARING come together

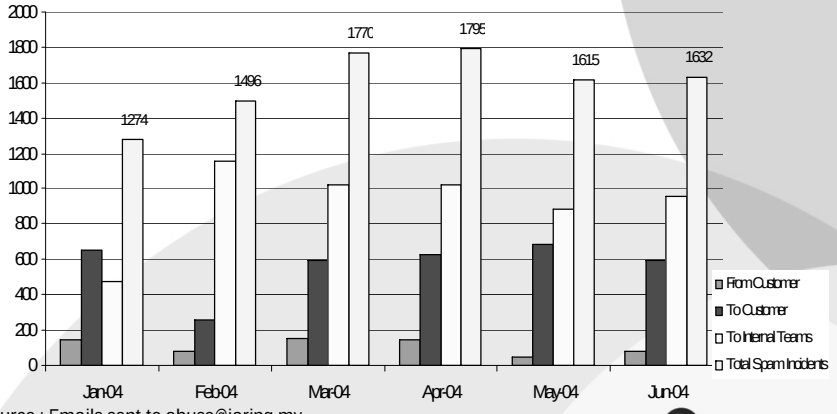
JARING Incident Reports (2004)



Source : Emails sent to abuse@jaring.my

JARING come together

JARING Spam Incident Reports (2004)



Source : Emails sent to abuse@jaring.my

JARING come together

Part IV: Lessons Learned

"Experience is a harsh teacher. It first gives you the test then the lesson."

What Really Happened?

- In February 2003, 4 new accounts started operating under 2 company names.
- 2 more accounts started operating in May and June 2003, each under 2 different companies.
- During these periods, spam complaints shot up, and each company were dealt with separately (given ample time to respond, 2nd chances, etc).
- We monitored and found out in July 2003 that all these companies are actually the same spammer using spam-vertised mode.
- Suspended them immediately, and started termination process.
- Finally removed from SPEWS October 2003.

How did we get delisted?

- Only people behind SPEWS knows.
- But what we did was:-
  - Trace spamvertizing accounts (6) to their root (identified as one spammer), and blacklist the person.
  - "Clean up" our networks from these accounts: Suspend+disconnect them immediately, then terminate them.
  - Renew AUP, improve and detail out antispam enforcements.
    - http://www.jaring.my/corporate/aup/index.html

JARING come together

I thought we are handling spam cases?

- Current processes were inadequate. Examples:-
  - Inadequate policy, its enforcements and awareness, especially to downstream providers / hosting companies.
    - Many customers are unaware of how to handle spamming cases in networks delegated to them
    - Some are not sensitive to spam, I.e. subscribe to spammers' services to promote their products and services
    - Meanwhile, antispam community, especially blocklist maintainers, push for ISPs to play much greater role in ensuring that all their customers networks are "spam-source-free". (i.e. no open relays, spammers, worm-infected hosts, etc).
  - Spammers are terminated, but able to register again.
    - Global spammer networks like Bullet9 possibly have agents in Malaysia, registering company names used to hop around JARING (and other ISPs) networks.

JARING come together

Action #1: AUP Review

- Previous AUP (Terms and Conditions):-
  - You agree not to use the Forums or any other service provided by JARING to:
    - b) Upload, post, e-mail, publish, transmit or distribute any material containing any unsolicited or unauthorized advertising, promotions, surveys, junk mail, chain letters, pyramid schemes, or any other form of solicitation of goods and services;
- Needed stronger emphasis and detail.
- Published and Enforced new AUP:-
  - http://www.jaring.my/corporate/aup/index.html

JARING come together

Action #2: Improve Enforcements (Part 1)

- Be strict:-
  - Terminate customers who are proven to spam at first proven record of spam, I.e. no second chances (Exceptions: genuine negligence such as open relay).
- Be thorough:-
  - Monitor posting in blocklists, NANAE and NANAS, and take action on them ASAP.
  - Maintain own terminated companies / CEOs / contact persons responsible for spammer accounts, to be used for background checks on each new account, and made available to public, or at least all downstream providers.

JARING come together

Action #2: Improve Enforcements (Part 2)

- Be proactive:-
  - Downstream providers / hosting companies must be required to employ at least the same standards as JARING in terms of abuse management and policy enforcements
  - Maintain awareness among the downstream admins, I.e. set up mailing list for abuse-related discussions and announcements.

Action #3: Review Registration Process

- Do background checks on ALL potential corporate customers:-
  - Check company details, profile, key persons, etc. against JARING blocklist database
  - Check for any current or past affiliation with major global spammers like bullet9 or others found in Spamhaus's ROKSO database.
- If potential customer is a provider / hosting company, ensure they are aware of their responsibilities etc. as in our AUP and abuse management policies.

Action #4: Technical Preventive Steps

- Re-arrange networks to distance different classes of users (avoid mixed dynamic and static ranges)
- For e-mail services: scan and remove as much malware and spam as feasibly possible at the e-mail gateway (MX) level, while minimizing false positives and provide as much control to the customer as feasibly possible.
- **Monitor smtp traffic for spikes and spam patterns, and alert standby personnel for verification. Block the spamming host if verified.**
- **Monitor other traffic and resources (e.g. newsgroups) for spam instances attributed to the ISP.**

JARING come together

Part V: Challenges and Propositions

JARING come together

Challenge #1: Spammers Are Still Here

- **JARING booted them out, but they move to other ISPs. Watch out! Check for your ISP range in blocklists.**

Spam prevention

- Spam filter
- Policies and framework
- Laws and regulation

Proposition #1: ISPs Unite Against Spammers

- Proposition: ISPs need to work together! Some suggestions of what we have to maintain:-
  - A shared resource among Asian ISPs, or at least among local ISPs, of blacklisted customers (companies, individuals, etc).
  - A shared “whitelist” networks (ISP architecture networks, for exceptions in each others' blocklists)
  - Publish ISP's dynamic IP range (for blocking certain activities such as direct-to-MX)
  - Raise awareness / enforce security on users (e.g. audit customer networks and notify).

JARING come together

Proposition #2: Stronger Antispam Legislation

- Stronger policies, e.g.:-
  - http://www.jaring.my/corporate/aup/index.html
- Proposition: Work with regulators to discuss ways to close holes exploited by spammers (after termination, registering as some other company under someone else's name).
- Include Spam as part of Cyber Crime.
- ISPs and regulators work together with international antispam efforts, to regain back the country's tarnished reputation w.r.t. Spam.

JARING come together

Proposition #3: Education, Education

- The actions outlined in new policies require educating every level within the ISP organisation:-
  - Enforcers
  - Sales
  - Technical
  - Downstream providers
  - End users
- Customer/User Education also vital: e.g. FAQs on spam and other security issues.
  - (http://www.jaring.my/corporate/aup/index.html)
- Raise awareness on other areas prone to spam (mobile, fax, phone, etc).

JARING come together

Thank You.

Mahizzan@jaring.my
Abuse@jaring.my

JARING come together