Shared Incident Response

towards mitigation of spam and net abuse

Suresh Ramasubramanian

Postmaster, Outblaze Limited

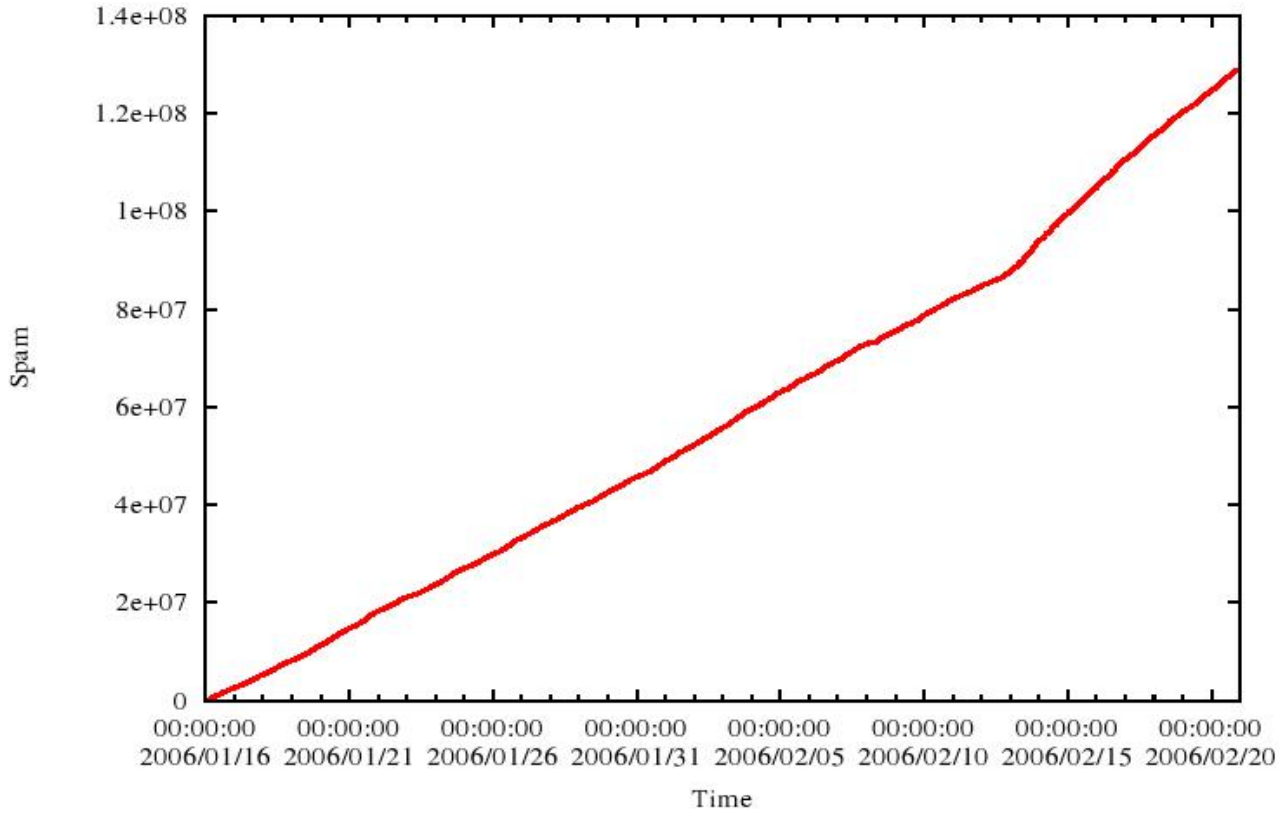
Coordinator, APCAUCE.ORG

Some quick background information

- Outblaze is a provider of hosted email and spam filtering
  - Over 40 million users around the world
- Ongoing spam metrics research project
  - In cooperation with Prof. Nick Feamster et al (Georgia Tech)
  - Some preliminary findings presented here
- Suggested action points based on these findings
  - *This is a work in progress, as are all antispam efforts*

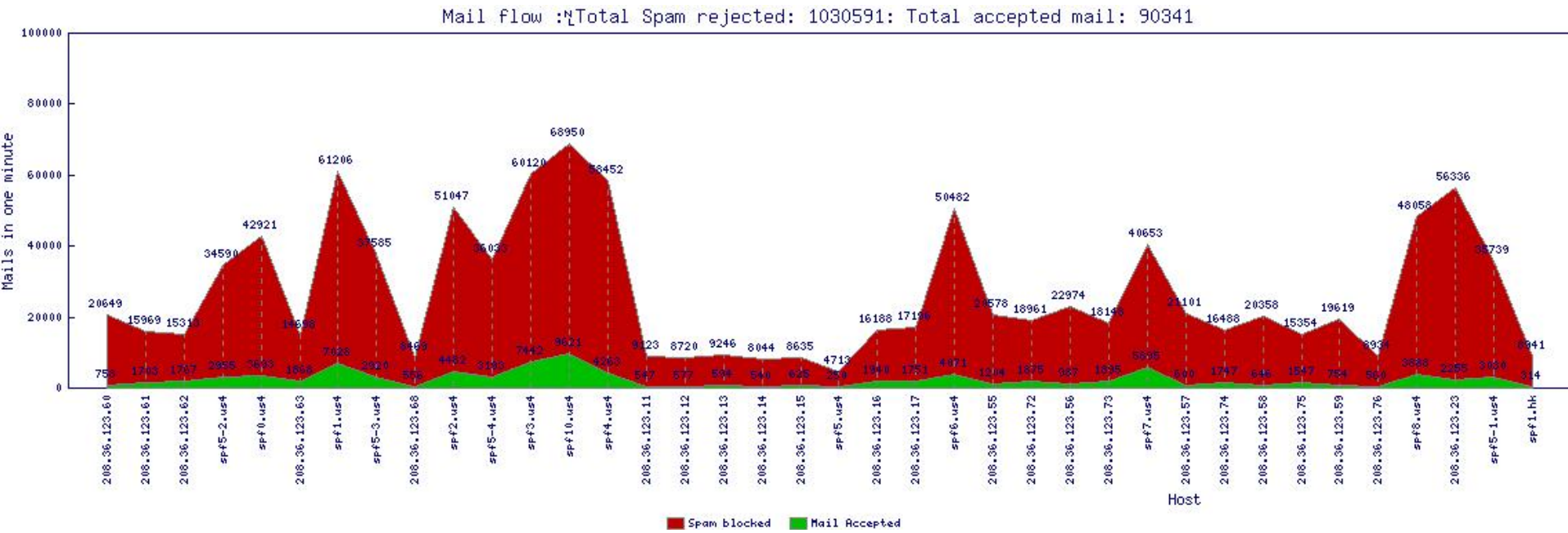
Consistently high volumes of spam

rejected SMTP connections over a week

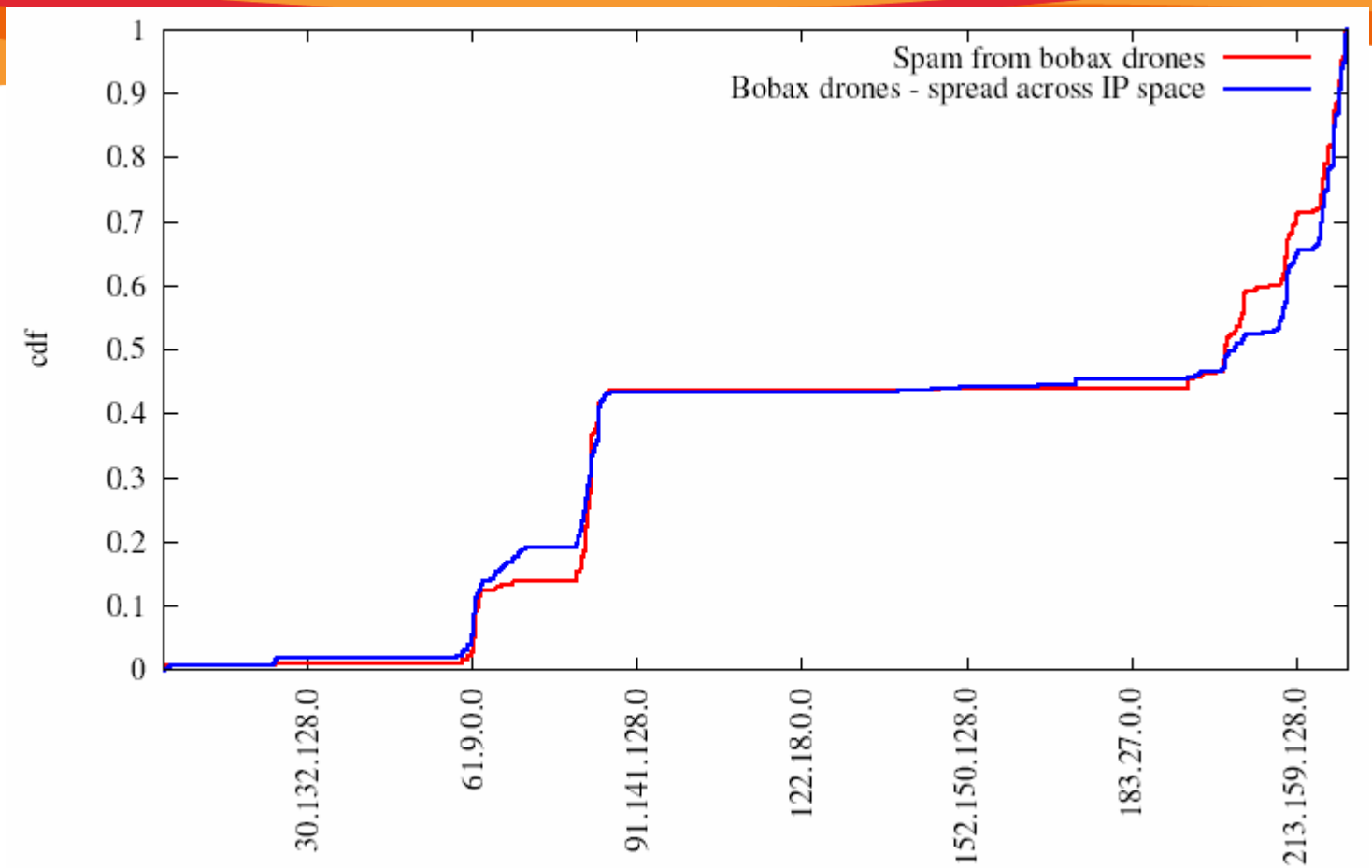


Spam far outweighs legitimate Email

one minute's worth of spam rejected v/s email accepted



Spam from “Bobax” infected hosts



Spam sources – by ISP

CHINANET-BACKBONE	7.61%
CHINA NETCOM - BACKBONE	5.05%
KOREA TELECOM	4.22%
TELEFONICA DEL PERU SAA	2.34%
TELEFONICA DATA ESPAÑA	1.68%
TPNET POLISH TELECOM	1.67%
TTNET TURK TELECOM	1.56%
VERIZON	1.53%
CHINANET-SH SHANGHAI	1.43%
AT HOME BENELUX (HOME.NL)	1.30%

Spam sources – by Country

United States of America	25.85%
China	17.68%
Korea, Republic of	06.73%
Russian Federation	03.83%
Poland	03.61%
France	03.12%
Spain	03.04%
Brazil	02.81%
Germany	02.47%
Peru	02.44%

Botnet Abuse

- Botnets have brought about an industrial revolution
- Net abuse now self contained and self perpetuating,
  - Viruses infect PCs, use them for Spam, DDoS etc
- Entire net abuse cycle now on botnets
  - Botnet command and control, malware distribution, DNS
  - Spam origins, DDoS vectors, warez / child porn archives
- Botnets change location and characteristics rapidly
  - From one infected PC to another [also hacked webservers]
  - Sometimes within minutes – “fast flux” hosting
  - Multiple redundancy, no single points of failure

Net Abuse / Spam Domains
a single point of failure

- Registered in bulk quantities, hundreds at a time
  - With bogus contact information and using stolen credit cards
    - namebworld.com, namecop.net, nameda.net, namedn.com
    - access-earthlink.com, compuserve-center.com, yahoo-home.net
- Domain registrars can help stop this
  - Proactive detection and deactivation of fraud / spam domains
  - This has to be rapid, possibly automated to have any effect
- Priority action items for antispam organizations
  - Outreach to domain registrars
  - Relevant inputs into the ICANN process
  - Promotion of antispam / net abuse policies among registrars, webhosts

419 Spam – moving with the times

- They don't always pretend to be relatives of dead dictators
  - An American soldier finds Saddam's hidden loot in Iraq
  - A priest at Pope John Paul II's deathbed learns the location of a hidden papal treasure
- They have diversified into money laundering and phishing
  - Buying goods online and paying with fake cards and checks
  - Recruiting mules to process stolen goods and money
  - Impersonating Citibank, the USPIS, Western Union, DHL etc
- And some even more innovative scams
  - An "FBI agent" emails scam victims, and extorts a bribe to not prosecute them for money laundering offences.
  - An "official of the US embassy in Nigeria" emails victims and accuses them of defrauding "reputable Nigerian businessmen".

Developments in Incident Response

- Filtering incoming net abuse is not enough.
  - Widespread recognition that “outbound spam” has to be dealt with
  - Shared reporting and enforcement mechanisms are necessary
    - Ensures quick, effective mitigation of spam and net abuse
- Widespread adoption of real time Incident Reporting mechanisms
  - Feedback Loops - inter-ISP spam reporting mechanism
    - Tied to “report as spam” buttons in email programs and on webmail
  - Standard, machine readable “Abuse Reporting Format”
    - http://www.mipassoc.org/arf/
    - Several ISPs including AOL, Outblaze, Earthlink etc., now offer ARF loops.
  - CERTs developing their own format (INCH)
  - Governments, Public – Private partnerships (SpamMatters, Signal Spam)

Future trends in Incident Response

- Consolidation and Cooperation
  - OECD, APECTEL, ITU, London Action Plan, Seoul Melbourne Pact
  - APCAUCE, MAAWG, e-COAT, FIRST Abuse SIG etc
- Integration of different incident reporting and response efforts
  - Several widely different efforts, that do not interoperate
  - Widespread reinvention of the wheel
- Outreach and Capacity Building efforts – Target “problem” areas
  - Reach out to relevant stakeholders, launch capacity building efforts
    - OECD Antispam TF – Spam Problems in Developing Economies
      - http://www.oecd.org/dataoecd/5/47/34935342.pdf
    - Additionally - law enforcement coordination with Nigeria, Eastern Europe etc ..

Coordinating with Law Enforcement

- Active cooperation with law enforcement in different countries
  - Balanced with the need to respect user privacy
  - In consonance with your existing policies and local laws
  - Reach out to law enforcement in problem locations as well
    - Contact established with the Nigerian EFCC during a conference in Abuja
  - Develop contacts with Industry anti fraud / phishing teams
- Law enforcement against Internet abusers requires quick reaction
  - Standardization of online contact mechanisms
  - Secure online transmission of subpoenas
    - Digitally signed emails instead of faxes or certified mail?
  - Personal equations with individual LE agents can be quite useful
    - But no substitute for standard points of contact

Thank You

suresh@outblaze.com