ISP-Security BOF

What security/abuse related tools you need to be a more effective NSP/ISP/ASP/xSP

The Internet now connects all parts of society from Kings and Presidents to Beggars and Thieves.

What tools do NSPs need?

- Machine processing of reporting formats
  - Abuse Reporting Format (ARF)
  - Incident Object Description and Exchange Format (IODEF)
- Tools to review and verify large numbers of incident reports
- Tools to assist large numbers of victims (notification, technical assistance, financial recovery, emotional support)
- Tools to prevent unwanted communications and technical intrusions (identification of sources, automatic updates of unmanaged systems, social policy in applications)

A few "Successes"

- eBay fraud team helping law enforcement arrest an average of 3.5 people per day world-wide
- Phishing sites last less than 5.5 days on average (some commercial protection firms claim 30 minute response)
- Several of the largest ISPs in the US are deploying subscriber notification and repeat offender escalation systems by 2008
- Changes to default configurations have reduced SMURF attacks, open SMTP relays (other attacks are now easier)
- Law enforcement in 50 countries have created a 24/7 assistance network for collection of electronic evidence (using or sharing the evidence after collection is still an problem)

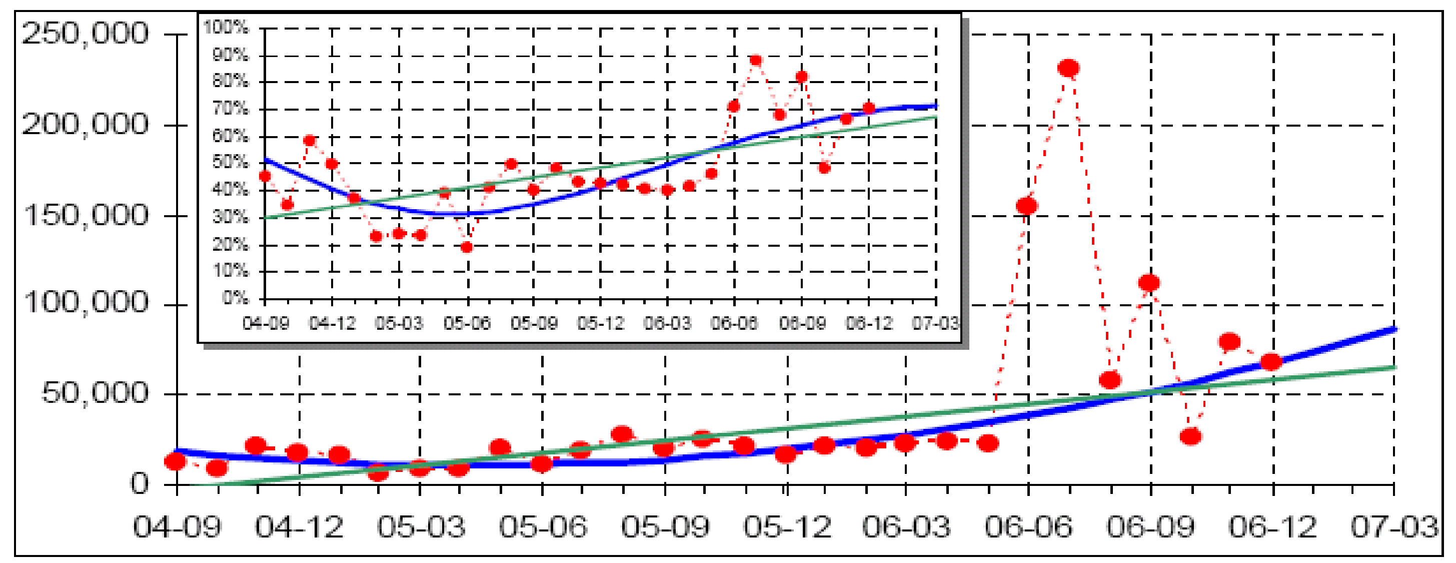
The scale of incident reporting

- A large ISP received (different years 2001-2006)
  - 4-6 million daily reports from public/subscribers
  - 1,000 criminal monthly requests
  - 30 civil monthly requests (90% legally defective)
- A large content owner (2006)
  - Made Over 1,000,000 DMCA complaints in 2006
- Spam reporting organization
  - Receives 11.6 submissions generates 21 complaints per minute
- Cyberbulling was reported to parents (50%), friends (33%), ISP (21%), teachers (6%) and LEA (1%)

Incident reports require analysis

9-1-1 Answering Points report 40%-60% of calls are not classified as emergencies after review

INHOPE – International Association of Internet Hotlines



Number of Processed Reports about Other Content or Content which is Not Illegal
and as a percentage of the total reports processed..

Responding to incidents

- One ISP spent 15% of its monthly fees responding to abuse/security incidents
- Estimates range from 5 minutes to 4 weeks to remediate a compromised system
  - Users don't believe/don't read e-mail, old contact information, the Internet is more than just Web
  - Human assistance is limited by the number of knowledgeable people available
- Some victims don't want to believe they were victimized (and security products they use miss stuff)
  - Do the tools actually find all the problems
- If original cause is not addressed, repeatedly re-compromised
  - Technical cause, Social cause, Criminal cause