# BotNet Mitigation Panel

# The Private Sector Attempts

- In the past year, having a botnet notification system is all the rage
  - ECO (Germany), Australia, REN-ISAC (US)
  - ISPs
- There is some regional efforts, too
- There are some remediation efforts, too
  - ISPs, and corporate CERTs
- Most of the current efforts are ‘national’ scope

# Are they successful/efficient?

- A botnet notification system has three parts:
  1. Botte/infectee/maluser detection
  2. Notification to IP Address space ‘manager’
  3. Remediation of infection

- All the techies want to do #1
  - i.e., find a zeus before zeustracker does. ☺
- S.T.C. may help with #3
- I think the big challenge is #2

# What's an APWG to do?

- [Discussions with members ensued]
- We're not going to run a detector system
  - But we have members
  - And we know a lot of "IP Address space Managers"
- Could we let our members send us infected IP addresses like we do phish URLs?
- We're working on a pilot idea (BISANS)
  - You send us stuff
  - We let you pull a list
  - and we notify the 'manager' of the IP address

# Thank you

- BISANS should be running before the end of the year.
  - We're holding off accepting large volumes of data until the back end notifier and search functions work
    - The data now just gets collected into a list
  - Feel free to send us test data via the previously mentioned scripts
- Write-up:
  - repoman.apwg.org/research/attachment/wiki/bisans/