VirtualBotmaster

http://sourceforge.net/projects/virtualbotmaster/

Goal & Architecture

- To generate simulated NetFlows based on real malware behaviors.

- One Botmaster Process
  - One Botnet Process
    - One Bot Process
      - Several CC Processes

Demo

Behavioral Models

- Flow-based
- 3-tuples
- 2nd time difference, duration, size.
- Markov Chain
- Store:
  - Matrix, initialization vector, state of letters, t1, t2, Paq/Bytes ratio, probability longest state, histograms of each letter.

NetFlows time, dur and size

- Use the MC to generate new states.
- Each state represent: time, dur, size.
- Select each value from its histogram.

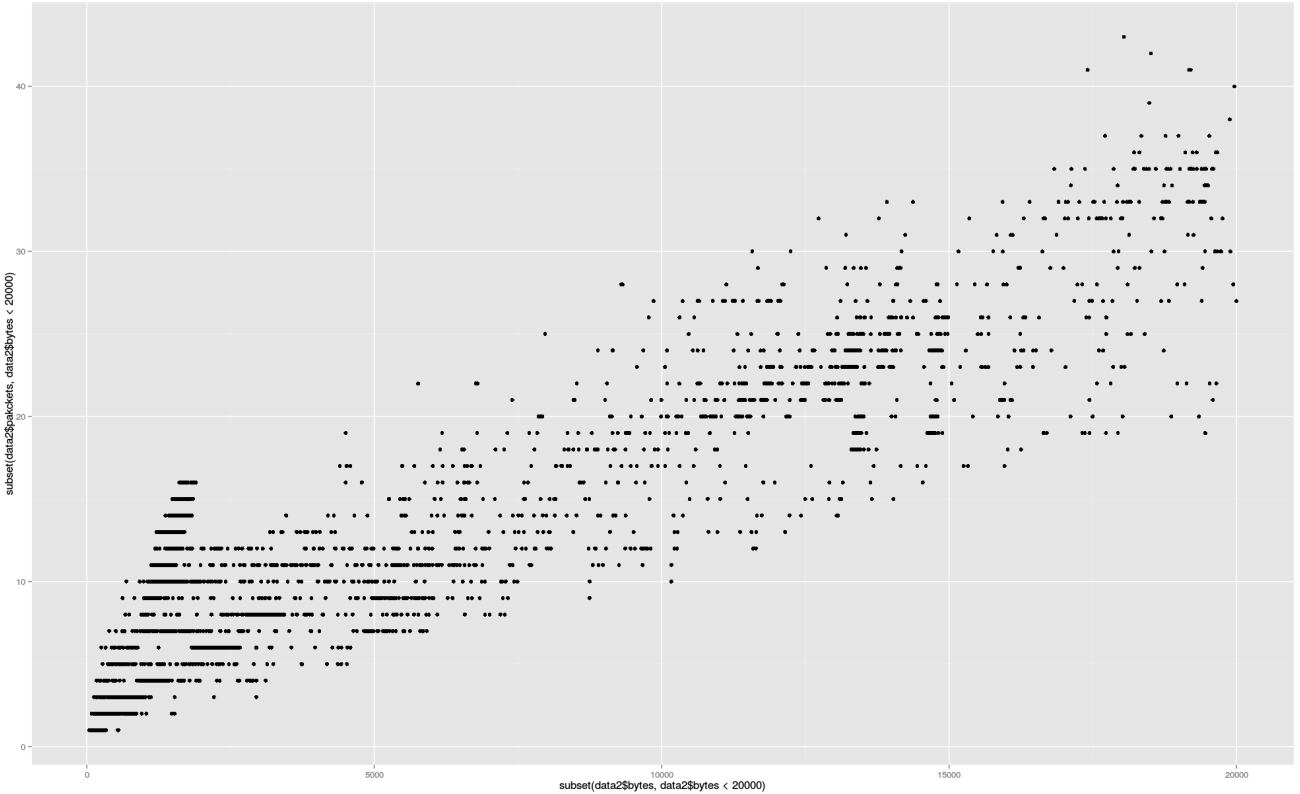
NetFlows source port

- Port ranges for Linux, WindowsXP, Windows7 and 8, Malware onWindows, and custom port.

NetFlows state

- Difficult. Uses argus standard but can be migrated.
- UDP are separated in established or attempts.
- TCP are always established with all the packets in one flow.
- No report time of the NetFlows yet!

NetFlows packets



NetFlows packets

- There is a relationship. We store the ratio for the model and apply it.
- Basic checkings: min packet 41 bytes, max 1500. Up to 120 bytes, uses 1 packet.

Generalization

Demo