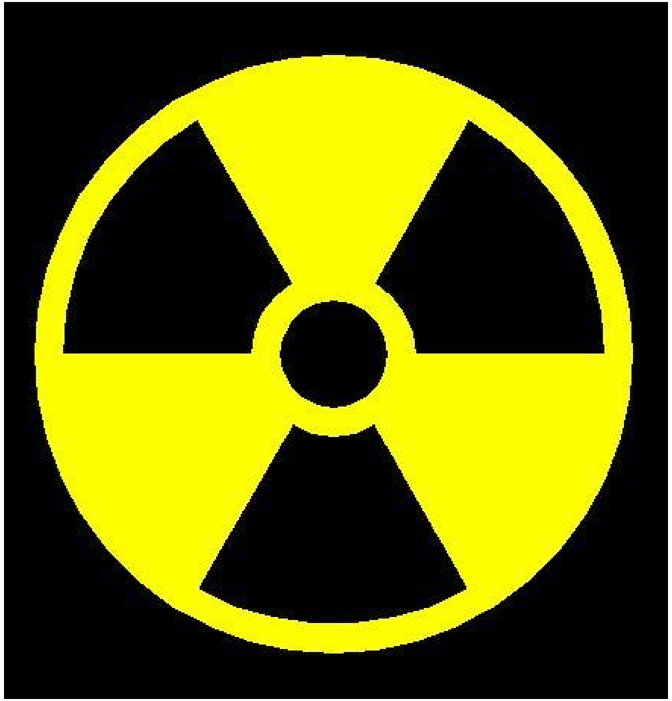
Internet Background Radiation

Classification and Characterisation

David Yates

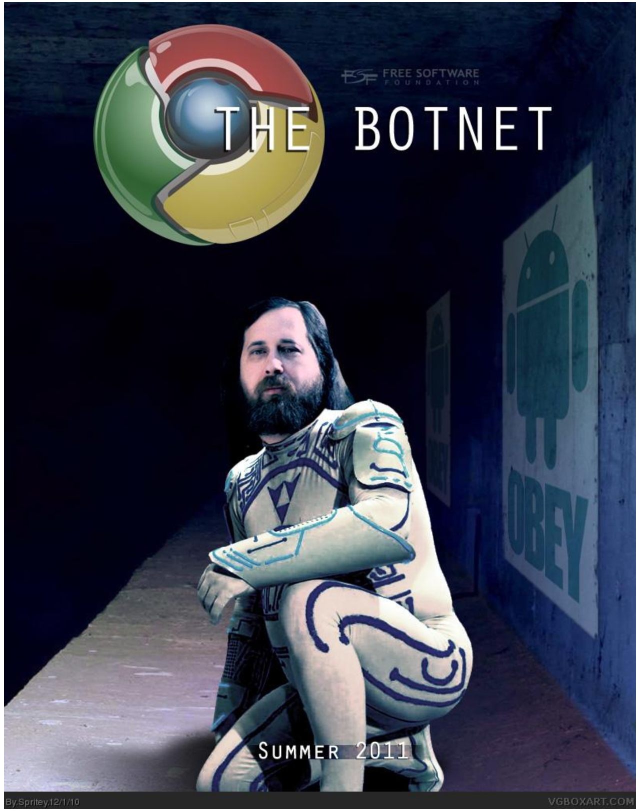
Supervised by Barry Irwin

What is IBR?



Main Components

- Reflected DDoS attacks
- Worms
- Botnets
- Misconfigured routers



History

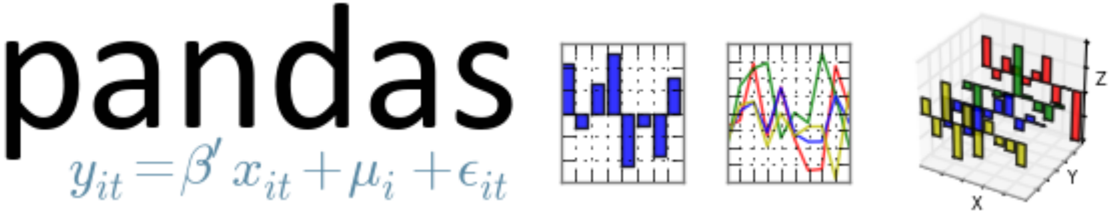
- Early Internet: no mentions of IBR
- Early-to-mid 2000s: IBR begins to be noticed
- 2008: Large increase of IBR after the advent of the Conficker worm

Similar Projects

- *Toward a Model for Source Addresses of Internet Background Radiation* – Barford *et al.* (2006)
- *Detecting BGP Route Information: Going Beyond Prefix Hijacking* – Qiu *et al.* (2007)
- *Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet* – Dainotti *et al.* (2012)

Approach

- Rhodes network telescopes
- Diurnal behaviour
- Packet ports
- Changes in traffic composition
- Using Python and Pandas



Possible Applications

- Sorting historical data
- Contribution towards a real-time DDOS, worm and botnet detection system
- Basis for generating similar traffic for simulation and further research

Questions!