Internet Background Radiation

Seminar in Distributed Computing

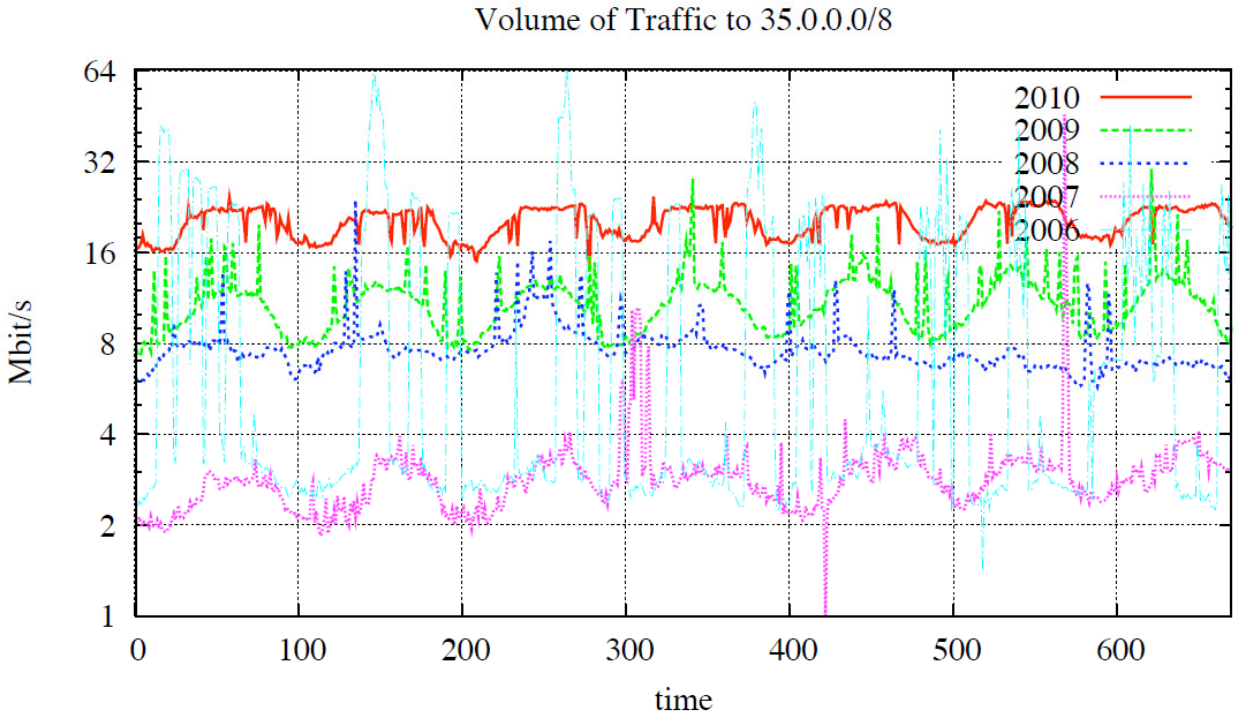
Jeremia Bär

Internet Background Radiation?

Network packets to unassigned addresses.

Useless Traffic

Why would I care?

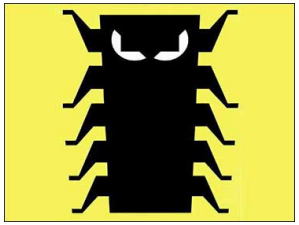


Internet Growth: 50% / annum IBR Growth: 100% / annum

Radiation Sources

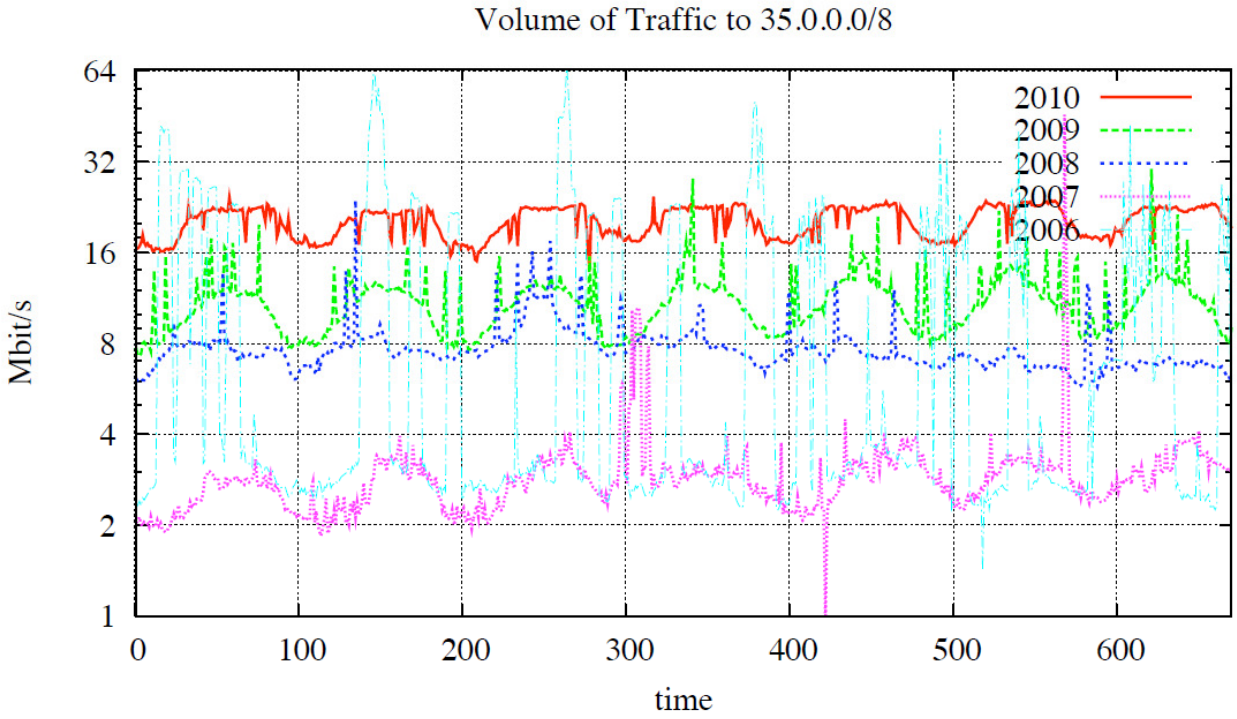
Computer Virus + Botnets

Hacking / DDoS



Software Bugs + Misconfiguration

Why would I care?



Internet Growth: 50% / annum IBR Growth: 100% / annum

Analysis Techniques

- Packet Analysis
- Temporal Analysis
- Spatial Analysis

Analysis Techniques

Packet Analysis
- Headers Analysis
- Payload Analysis

allows
- Application Identification
- Application Popularity
- Source OS

Temporal Analysis
- Analysis of (src,dst) pairs
- Cross-port analysis

allows
- Reveal Hidden Intention

Spatial Analysis
- Source Synchronization
- Network Avoidance

allows
- Software Maturity

Packet Analysis

Approach
- Header Analysis
- Payload Analysis

Results
- Application Identification
- Application Popularity
- Originating OS

Temporal Analysis

Approach
- Analyse (src, dst) pairs
- Cross-port analysis

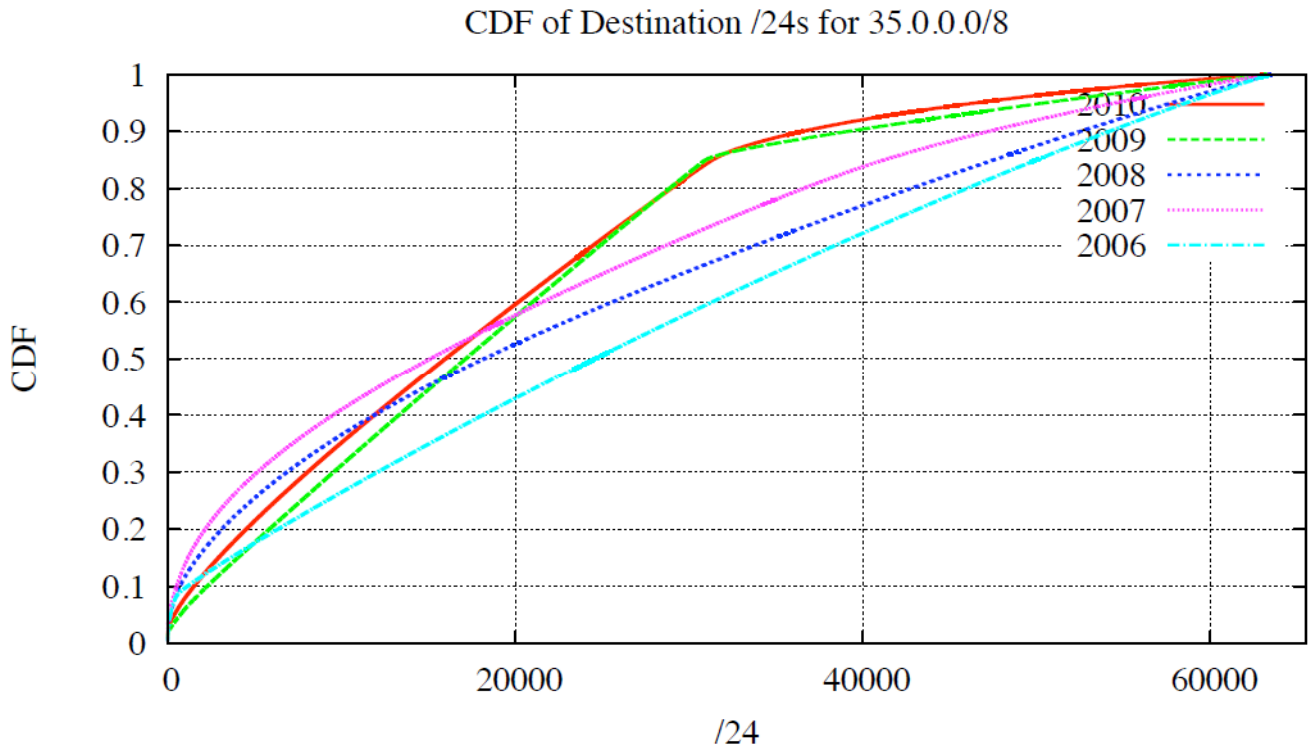
Results
- Identify Source Intention

Spatial Analysis

Approach
- Source Synchronization
- Network Avoidance

Results
- Software Maturity

Spatial Analysis



Focus due to Software Bug

Software Misconfiguration

Vendor bug in DSL Modem

Traffic to 1.x.168.192

Traffic to 35.206.63.212

Focused
Automated
No Control

Address Space Pollution

Summary

- Existance & Importance
- Packet, Temporal and Spatial Analysis
  - Classification & Filtering
  - Study of Malware
- Address Space Pollution

Up Next

- Measurement of IBR
- Real-world Applications

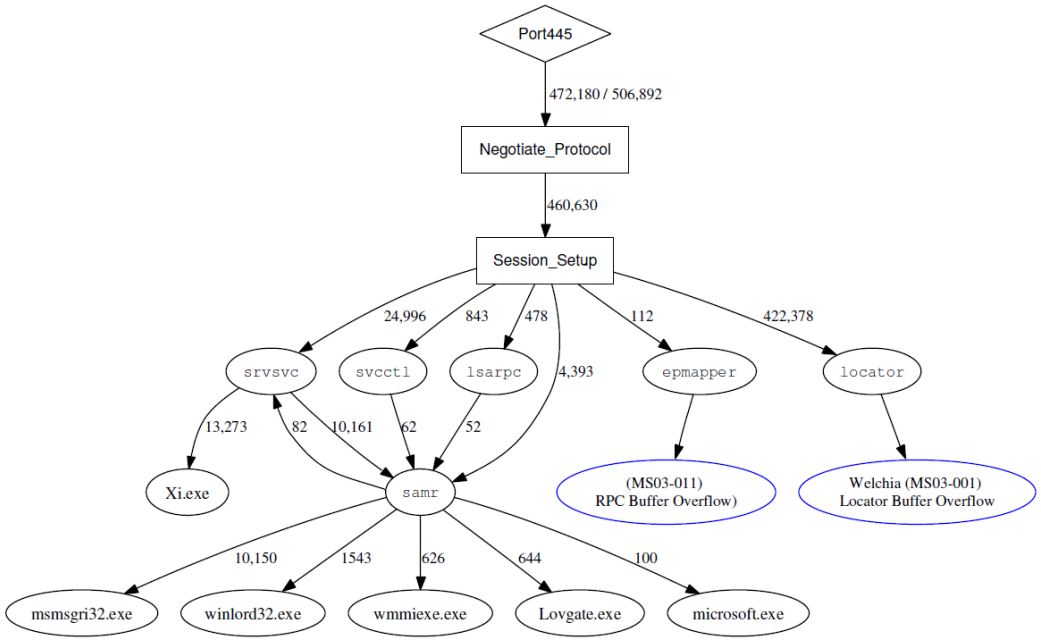
Measuring IBR

Measuring IBR

Darknets

Black Holes

Active Responder Complexity




```
-> SMB Negotiate Protocol Request
<- SMB Negotiate Protocol Response
-> SMB Session Setup AndX Request
<- SMB Session Setup AndX Response
-> SMB Tree Connect AndX Request,
      Path:  \\XX.128.18.16\IPC$
<- SMB Tree Connect AndX Response
-> SMB NT Create AndX Request, Path: \samr
<- SMB NT Create AndX Response
-> DCERPC Bind: call_id: 1 UUID: SAMR
<- DCERPC Bind_ack:
-> SAMR Connect4 request
<- SAMR Connect4 reply
-> SAMR EnumDomains request
<- SAMR EnumDomains reply
-> SAMR LookupDomain request
<- SAMR LookupDomain reply
-> SAMR OpenDomain request
<- SAMR OpenDomain reply
-> SAMR EnumDomainUsers request
```

Now start another session, connect to the SRVSVC pipe and issue NetRemoteTOD (get remote Time of Day) request

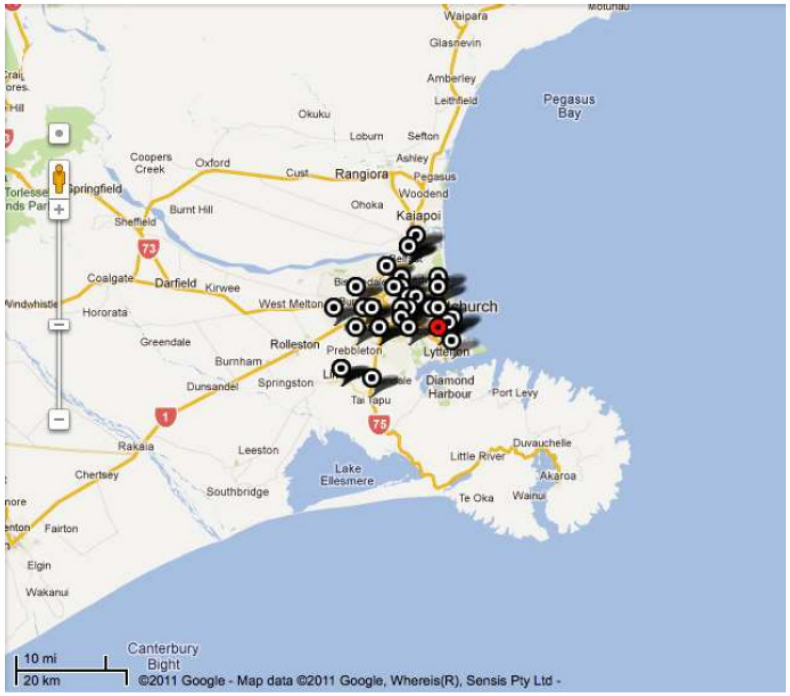
```
-> SMB Negotiate Protocol Request
<- SMB Negotiate Protocol Response
-> SMB Session Setup AndX Request
<- SMB Session Setup AndX Response
-> SMB Tree Connect AndX Request,
      Path: \ \XX.128.18.16\IPC$
<- SMB Tree Connect AndX Response
-> SMB NT Create AndX Request, Path: \srvsvc
<- SMB NT Create AndX Response
-> DCERPC Bind: call_id: 1 UUID: SRVSVC
<- DCERPC Bind_ack: call_id: 1
-> SRVSVC NetrRemoteTOD request
<- SRVSVC NetrRemoteTOD reply
-> SMB Close request
<- SMB Close Response
```

Now connect to the ADMIN share and write the file

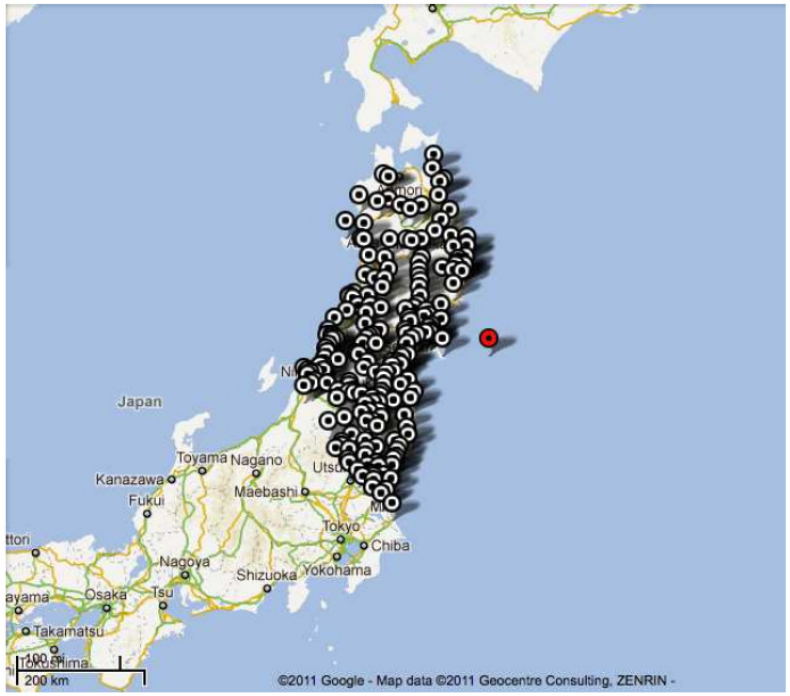
```
-> SMB Tree Connect AndX Request, Path: \\XX.128.18.16\ADMIN$
<- SMB Tree Connect AndX Response
-> SMB NT Create AndX Request,
    Path:\system32\msmsgri32.exe  <<<===

<- SMB NT Create AndX Response, FID: 0x74ca
-> SMB Transaction2 Request SET_FILE_INFORMATION
<- SMB Transaction2 Response SET_FILE_INFORMATION
-> SMB Transaction2 Request QUERY_FS_INFORMATION
<- SMB Transaction2 Response QUERY_FS_INFORMATION
-> SMB Write Request
....
```

Real-world Applications



Christchurch, NZ. 22.Feb. 2011
Magnitude: 6.1

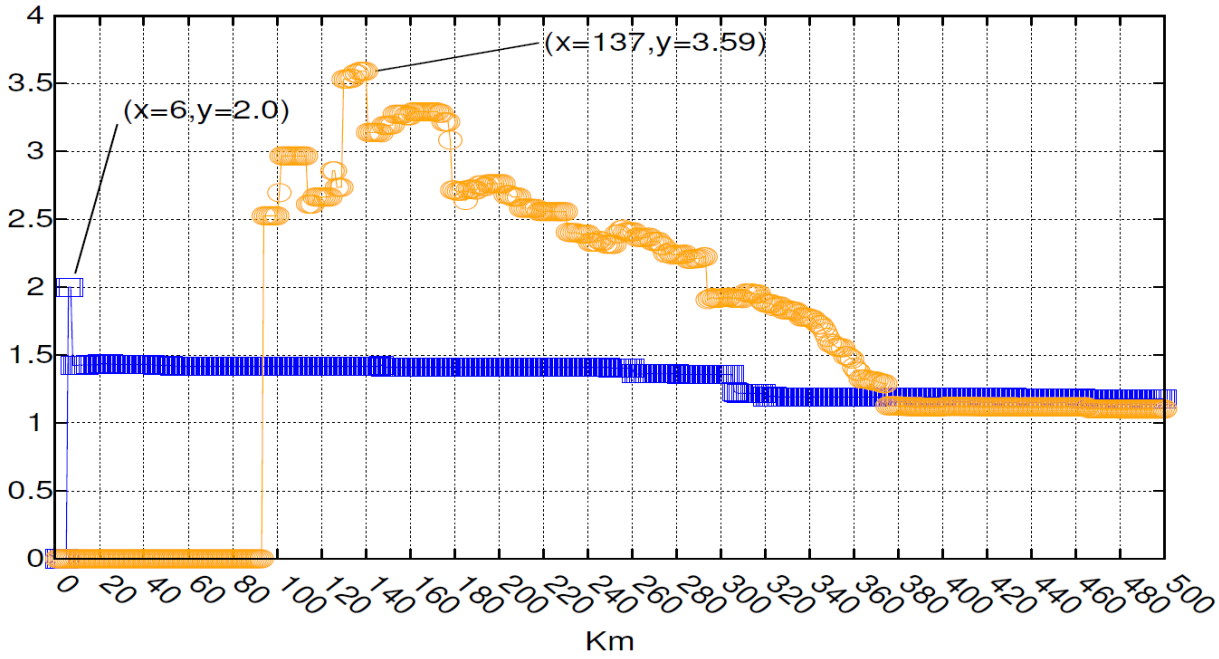


Tohoku, JP. 11. Mar. 2011
Magnitude: 9.0

Infrastructure Impact

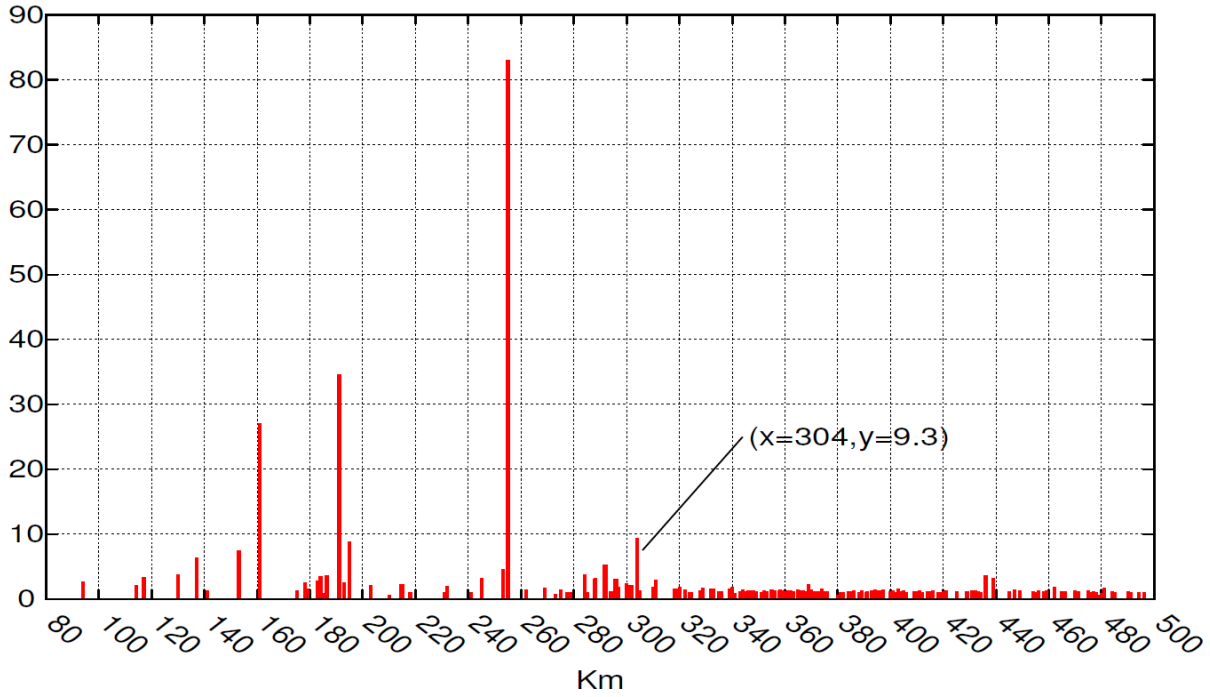
- Δt_i hour i from event
- $I_{\Delta t_i}$ distinct IPs observed

$$\theta = \frac{\sum_{i=-1}^{-24} I_{\Delta t_i}}{\sum_{j=1}^{24} I_{\Delta t_j}}$$



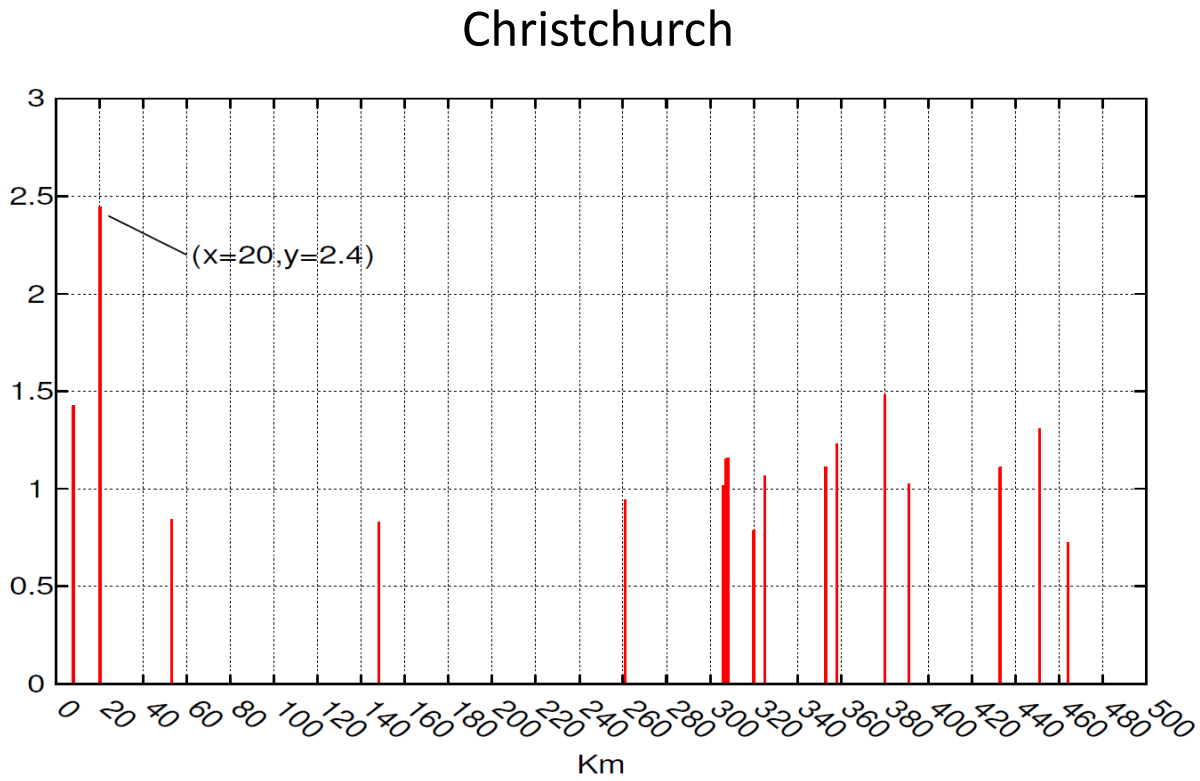
Infrastructure Impact

Tohoku



$$\theta = \frac{\sum_{i=-1}^{-24} I_{\Delta t_i}}{\sum_{j=1}^{24} I_{\Delta t_j}}$$

Infrastructure Impact

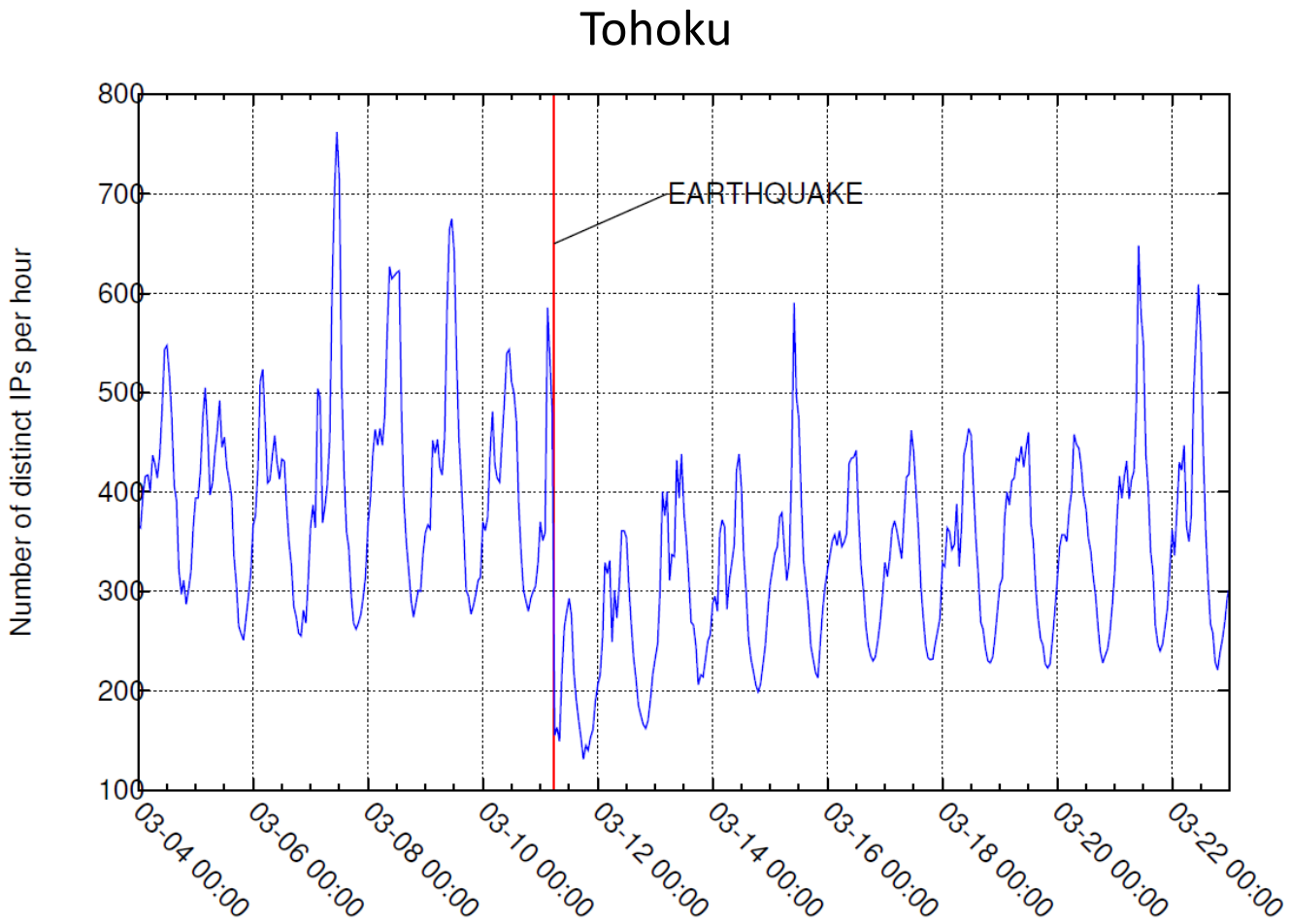


$$\theta = \frac{\sum_{i=-1}^{-24} I_{\Delta t_i}}{\sum_{j=1}^{24} I_{\Delta t_j}}$$

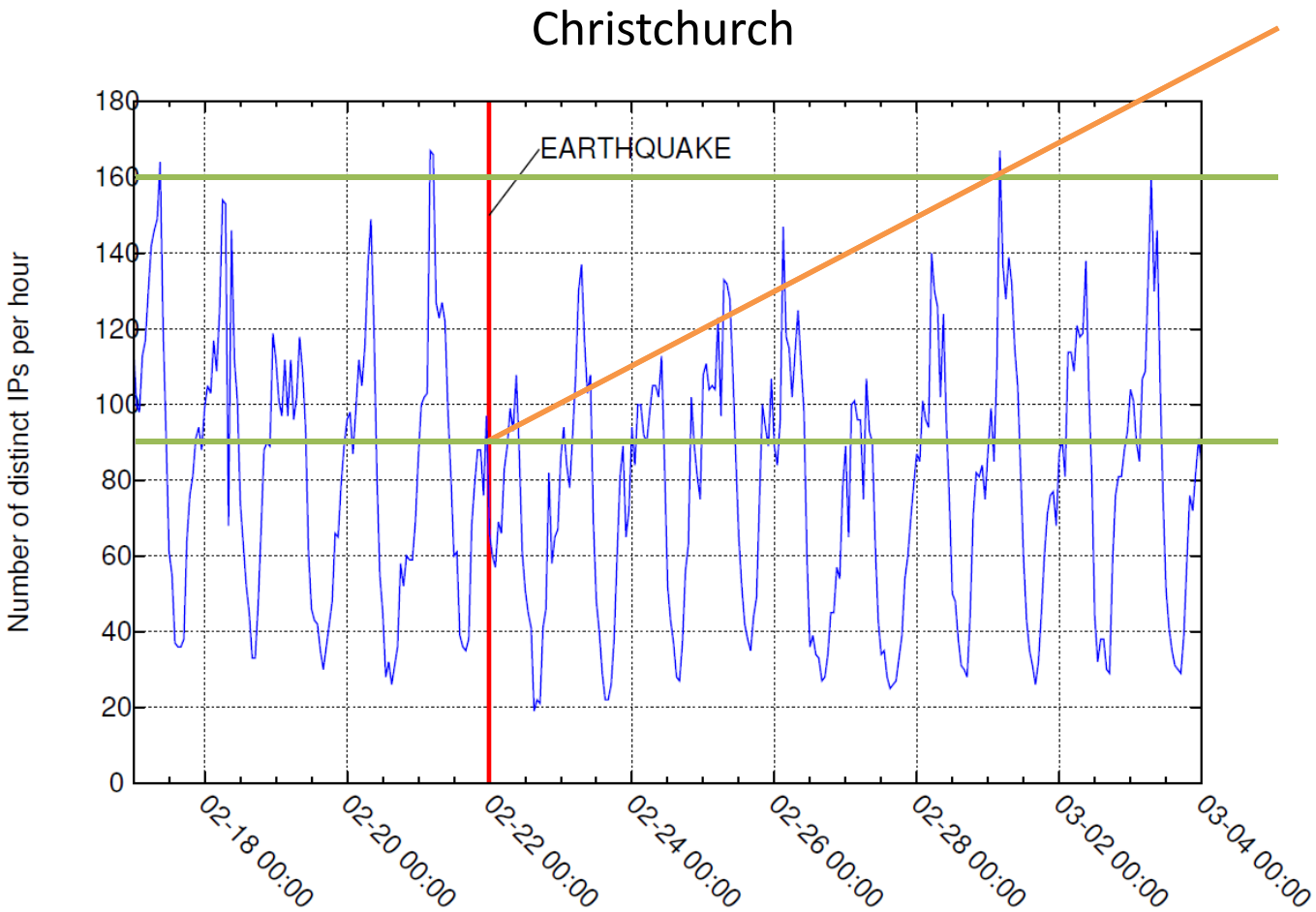
Infrastructure Impact

Property	Christchurch, NZ	Tohoku, JP
Magnitude	6.1	9.0
Impact Radius ρ_{max}	20km	304km
Impact Magnitude θ_{max}	2 (6km)	3.59 (137km)

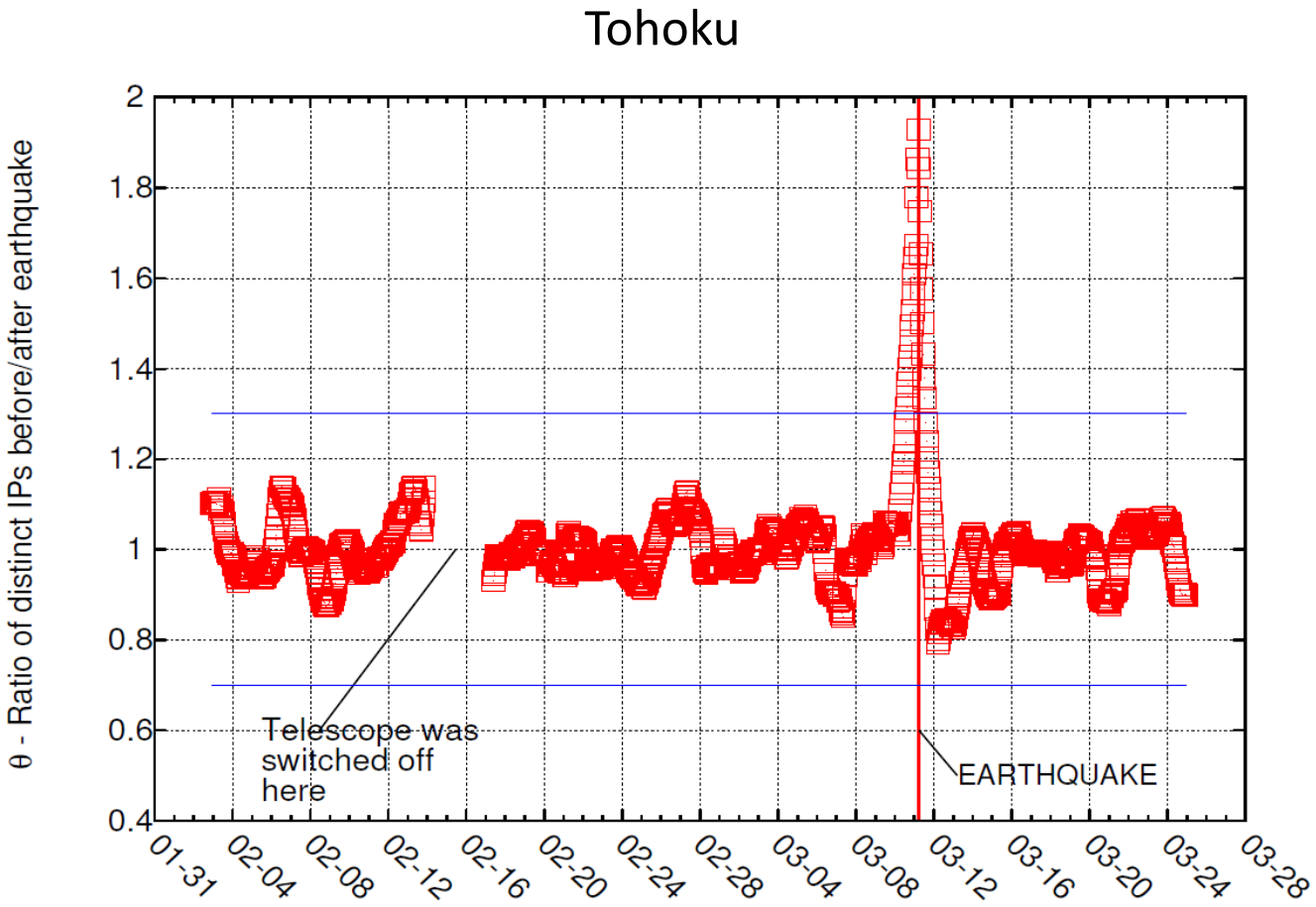
Long-term Impact



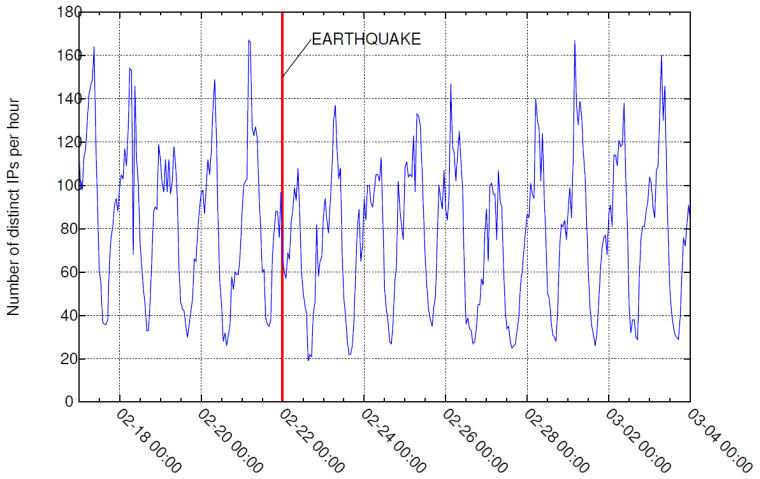
Long-term Impact

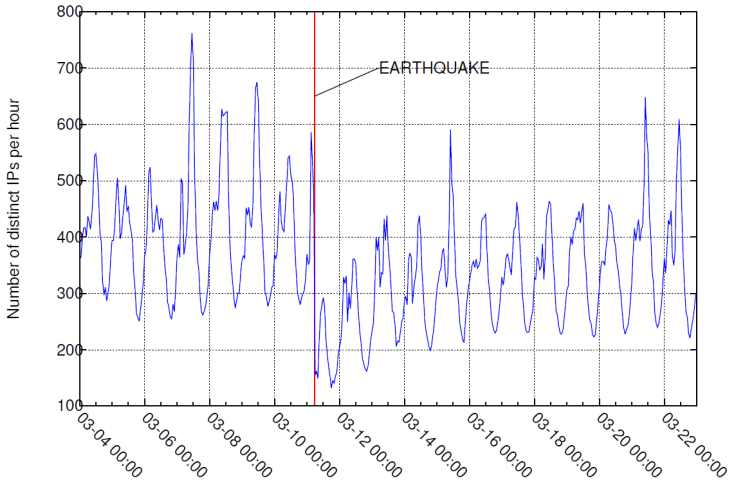


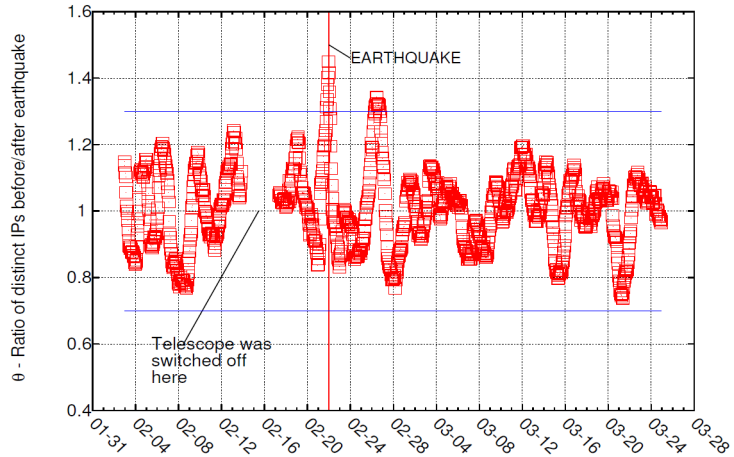
Reliability

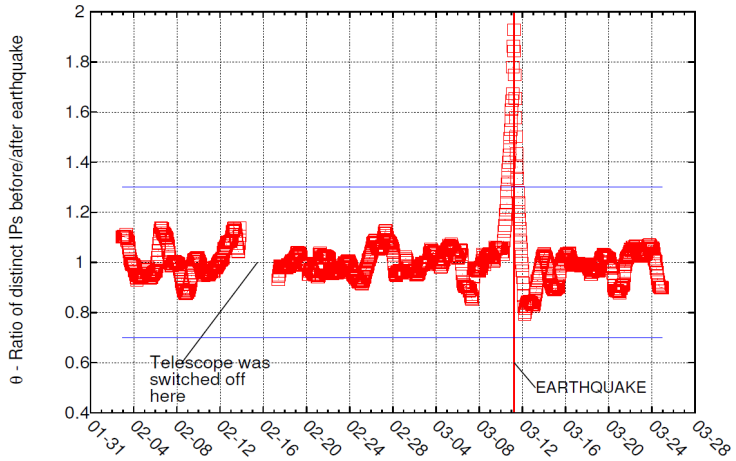


Big Scope & Recovery









Reliability

- Law enforcement
- ISP filtering
- Software Patches

- System Damage
- Accuracy of Geolocation
  - Mobile Devices

Summary

- Existance & Analysis
  - Packets, Temporal, Spatial
- Measurement
  - Darknets, Active Responders
- Tech Applications
  - Classification, Malware, Address Space Pollution
- Geographic Colocation
  - Communication Infrastructure Metric

Thank You

- *Characteristics of Internet Background Radiation.*
  Pang et al. In SIGCOMM 2004
- *Internet Background Radiation Revisited.*
  Wustrow et al. In SIGCOMM 2010.
- *Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet.*
  Dainotti et al. In SIGCOMM 2012.