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

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

Now connect to the ADMIN share and write the file
Real-world Applications

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

Magnitude: 9.0
Infrastructure Impact

- $\Delta t_i$: 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

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

(x=304, y=9.3)
Infrastructure Impact

Christchurch

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

(x=20, y=2.4)
## Infrastructure Impact

<table>
<thead>
<tr>
<th>Property</th>
<th>Christchurch, NZ</th>
<th>Tohoku, JP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Magnitude</strong></td>
<td>6.1</td>
<td>9.0</td>
</tr>
<tr>
<td><strong>Impact Radius $\rho_{\text{max}}$</strong></td>
<td>20km</td>
<td>304km</td>
</tr>
<tr>
<td><strong>Impact Magnitude $\theta_{\text{max}}$</strong></td>
<td>2 (6km)</td>
<td>3.59 (137km)</td>
</tr>
</tbody>
</table>
Long-term Impact

Tohoku

Internet Background Radiation,
Jeremia Bär, 2. April 2014
Long-term Impact

Christchurch

Number of distinct IFs per hour

Internet Background Radiation,
Jeremia Bär, 2. April 2014
Reliability

Tohoku

θ - Ratio of distinct IPs before/after earthquake

Telescope was switched off here

EARTHQUAKE
Big Scope & Recovery

Internet Background Radiation, Jeremia Bär, 2. April 2014
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