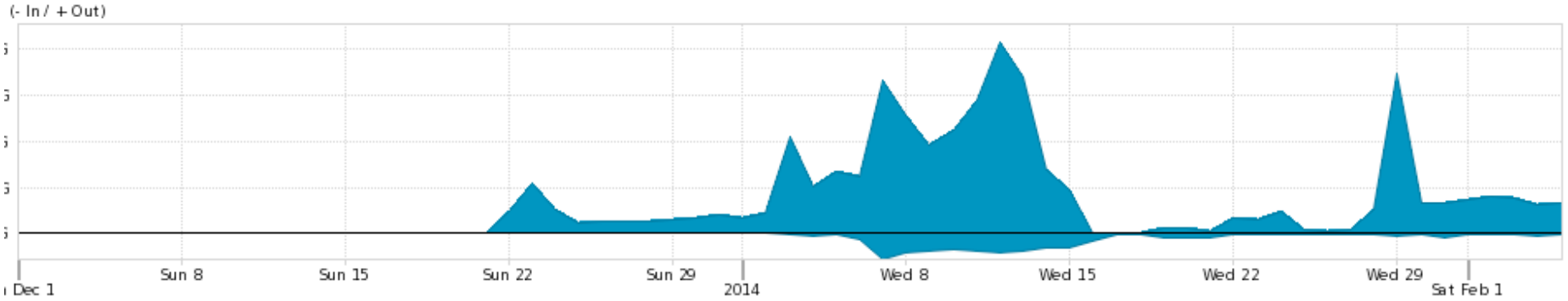
NTP Amplification Attacks

Jared Mauch, NTT
Manish Karir, DHS/CSD

Background

- Recently some of you might have seen NTP volume graphs in your networks that might have looked something like this:



Dec 1 Jan 1 Feb 1

Background

- Well understood and documented mechanism
- CERT Vulnerability Note VU#348126
  - http://www.kb.cert.org/vuls/id/348126
  - NIST CVE: CVE-2013-5211
- Amplification is a result of single small query to older versions of NTP servers that result in a potentially large list of hosts being returned to the requester

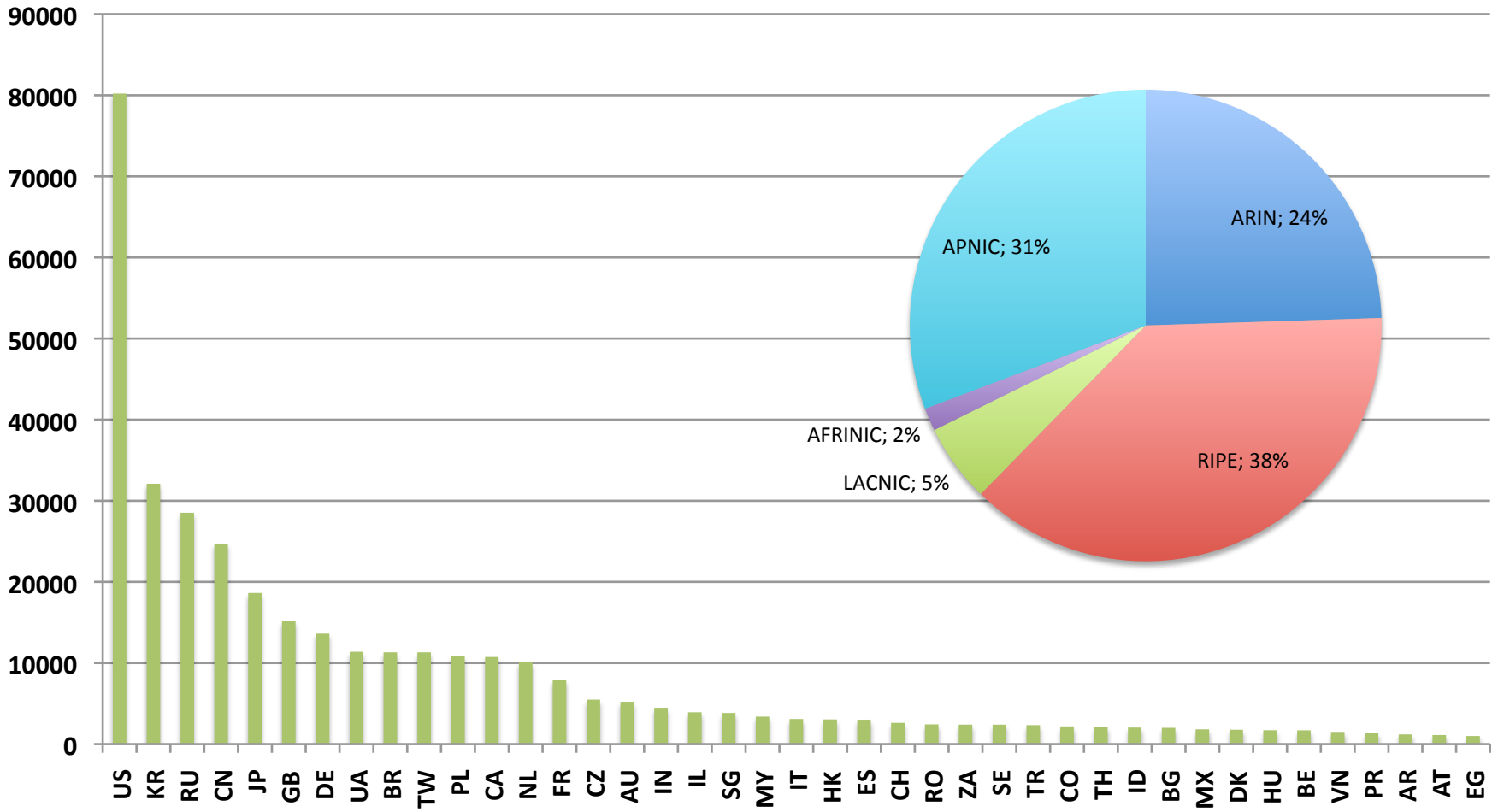
OpenNTPProject.org

- Methodology:
  - Send one packet to every IP to test if it generates a NTP MONLIST MODE 7 response
  - Once per week
  - Measure not only response result but also bytes returned – potential severity

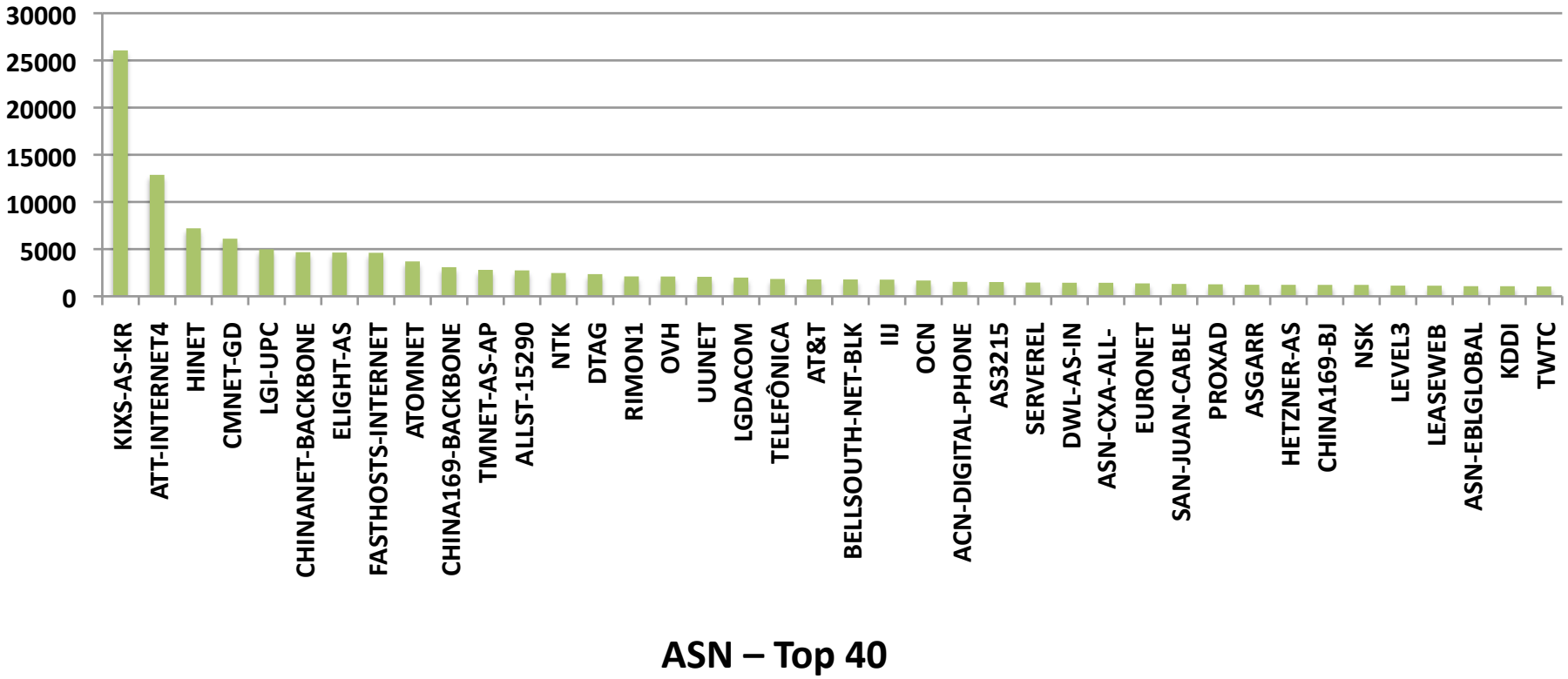
Preliminary Data Analysis

- Feb 7 2014 dataset
- 400K-500K unique IPs responded
- 13K unique ASNs
- Globally distributed across the 3 major RIR regions – LACNIC has fewer population
- US alone has 80K IPs (multiple ASNs) that responded over 30K from KR (most from single ASN)

Global View – Unique IPs

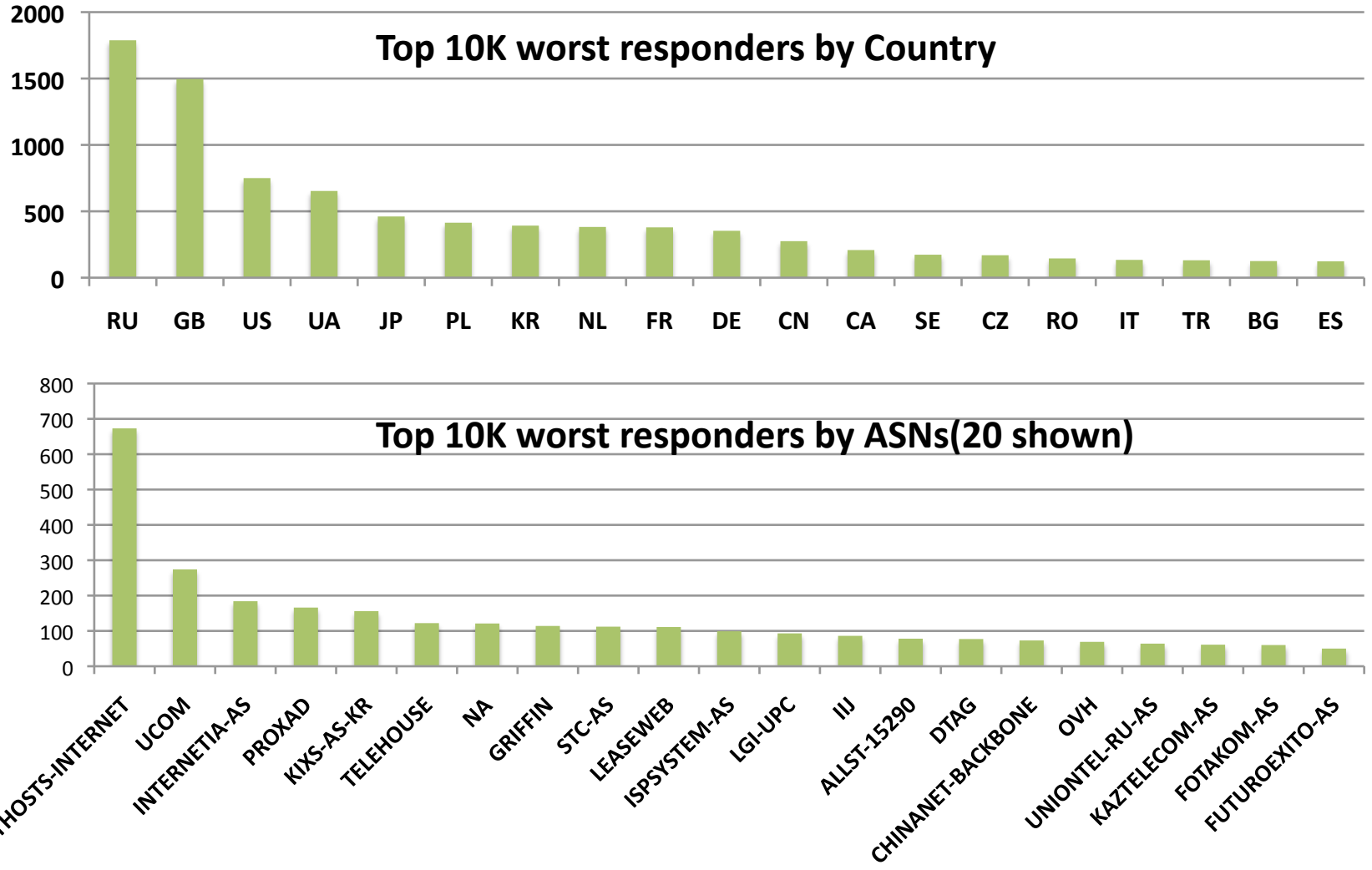


Internet View - ASNs



ASN – Top 40

Misuse Potential



Misuse Potential

- Top IPs from 2014-02-07 dataset, # of Bytes

61.122.x.x	21M
61.122.x.x	21M
61.122.x.x	23M
61.122.x.x	23M
70.62.x.x	24M
61.122.x.x	25M
87.255.x.x	54M
133.50.x.x	122M
133.50.x.x	1,5G
180.214.x.x	57G

Improving situation over time?

- Number of Unique IPs responding:

1529866	2014-01-10
1402569	2014-01-17
803156	2014-01-24
564027	2014-01-31
490724	2014-02-07

Conclusions

- Vulnerable population is available globally
  - Some specific concentration hotspots in terms of ASNs
- More important to understand the misuse potential in addition to the population at large – magnitude
- We see different results when we examine the magnitude
- NTP vulnerability has been fixed in newer versions of the software
  - upgrade to NTP-4.2.7p26 or later
- There are configuration fixes as well:
  - You can add disable monitor to your ntp.conf and restart your NTP process
- The server should also not respond to loopinfo or iostats requests as well