RIPE

DDoS Attack Trends Through 2009-2011

Yaroslav Rosomakho
Senior Channel Consulting Engineer, EMEA
Arbor Networks

RIPE

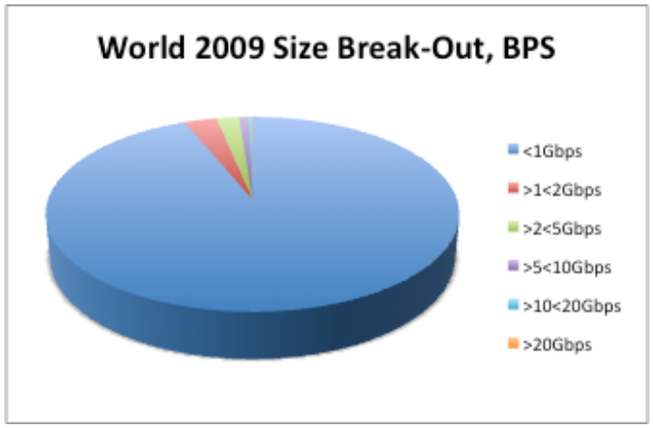
The Arbor ATLAS Initiative: Internet Trends

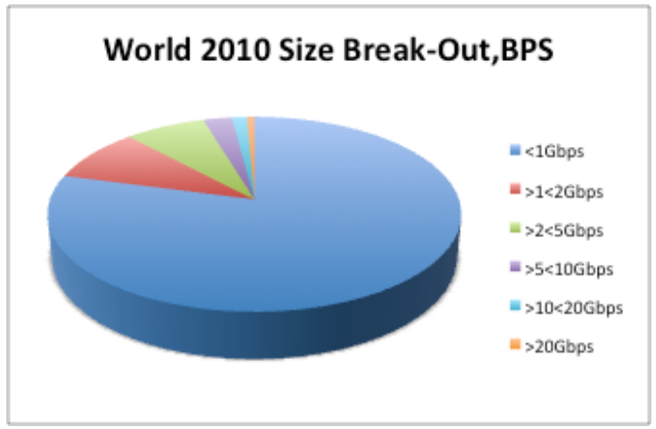
- 180+ ISPs sharing real-time data - > ATLAS Internet Trends
  - Automated hourly export of XML file to Arbor server (HTTPS)
  - File is anonymous, only tagged with
    - User Specified Region e.g. Europe
    - Provider Type (self categorized) e.g. Tier 1
    - Source / Destination addresses from within each participating customer are obfuscated.
  - Data derived from Flow / BGP / SNMP correlation
  - Arbor Peakflow SP product
    - Correlates Sampled Flow / BGP in real-time
    - Distributed in nature
    - Network / Router / Interface etc. Traffic Reporting
    - Threat Detection (DDoS / infected sub)
      - Multiple detection mechanisms

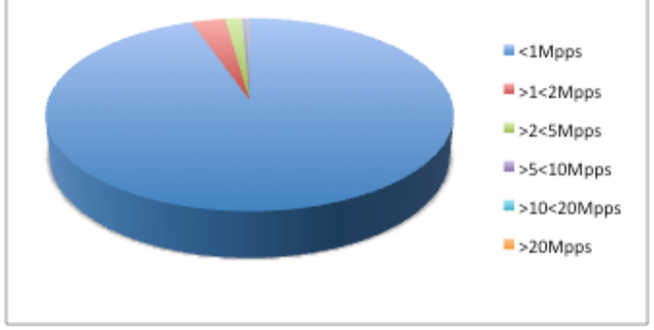
2010 ATLAS Initiative: Internet Trends, World-Wide

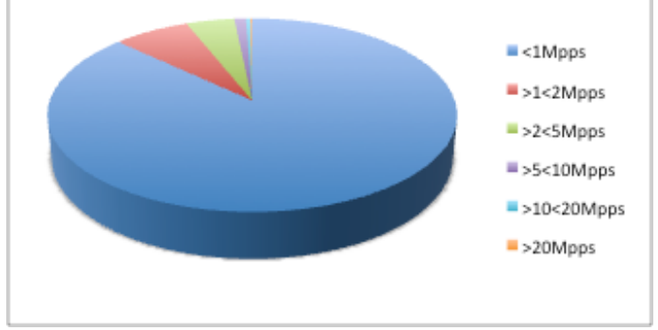
Small Attacks Continue to Make Up the Majority

- In 2010 most attacks still small:
  - 79% less than 1Gb/sec (down from 93% in 2009)
  - 87% less than 1Mpps (down from 94% in 2009)
- Average size of attacks
  - Less than 1Gb/sec:
    - 2010 is 197.41Mbps / 307.72Kpps
  - Less than 1Mpps:
    - 2010 is 558.96Mbps / 228.139Kpps







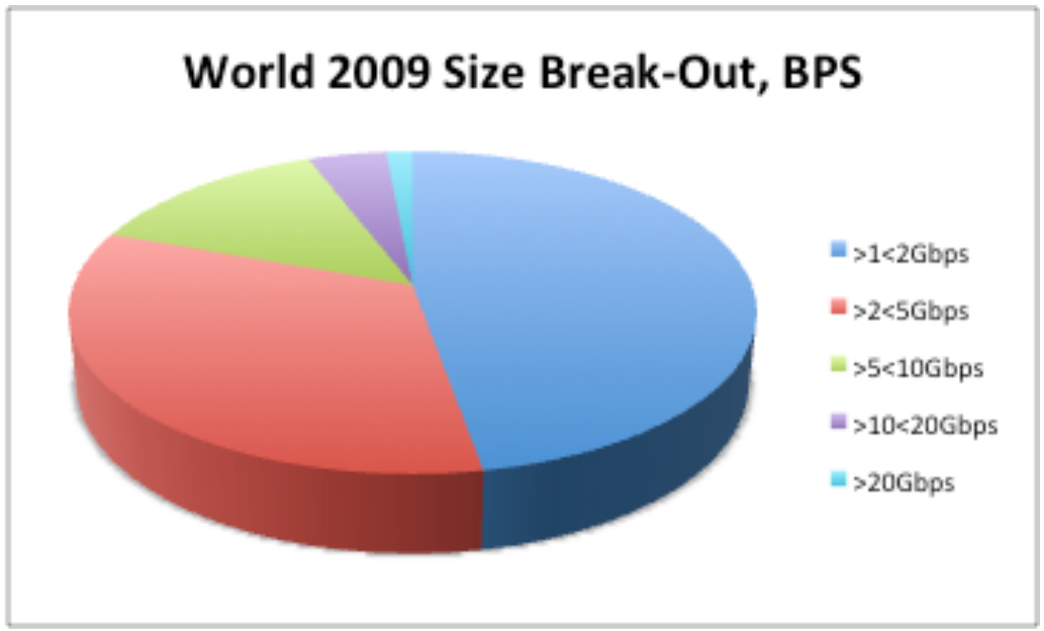


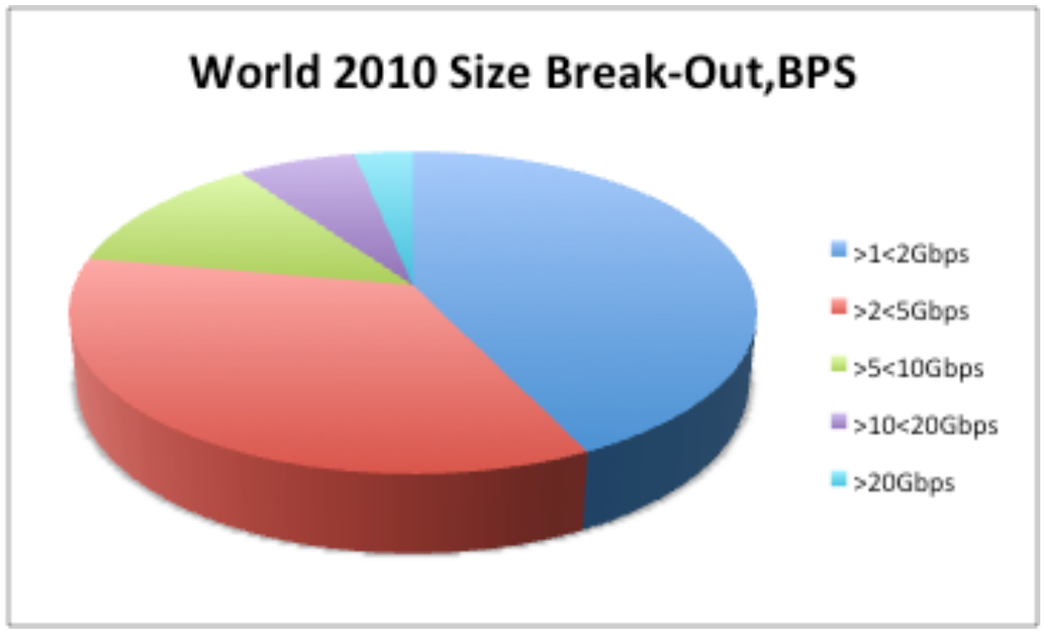
- Average attack sizes:
  - 2009 – 335.11Mbps / 290.17Kpps
  - 2010 – 1.08Gbps / 608.32Kpps

2010 ATLAS Initiative: Internet Trends, World-Wide

Attacks over 10Gb/sec on the rise!

- Proportion of monitored attacks over 10Gb/sec grew by 470% from 2009
- Proportion of monitored attacks over 10Mpps grew by 45% from 2009
- Increase in large bps / pps attacks year on year:
  - 319% increase in number of monitored attacks > 10Gbps from 2009 – 2010.



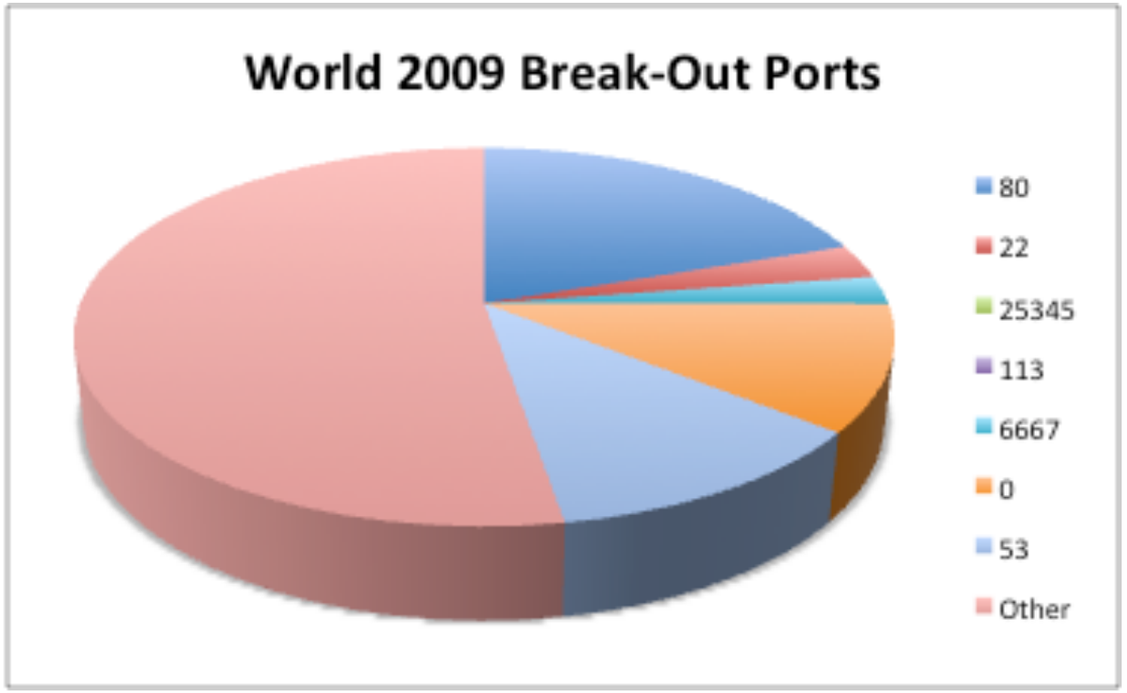


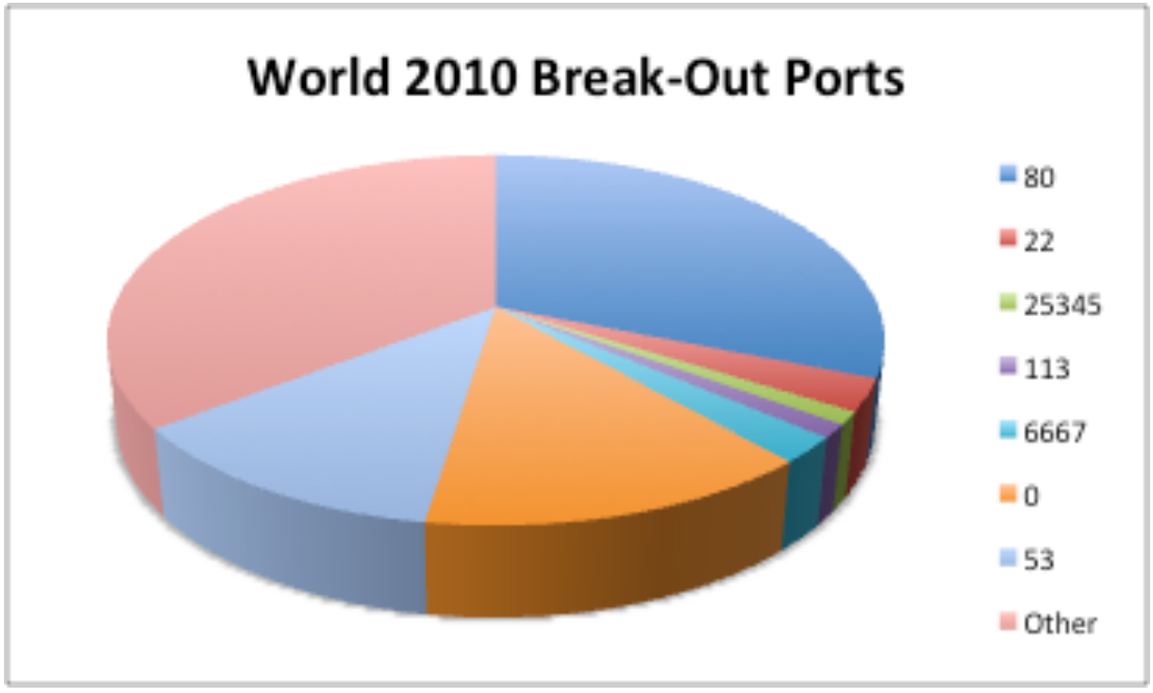
2010 ATLAS Initiative: Internet Trends, World-Wide

Proportion of Attacks Targeting Port 80 Increase

- In 2009, 19.6% of monitored attacks targeted port 80.
- In 2010 this had increased to 31%.

- Attacks targeting fewer ports
  - 80, 53 and Fragment
- Nearly 597% growth in number (474) of attacks over 10Gb/sec, targeting port 80.

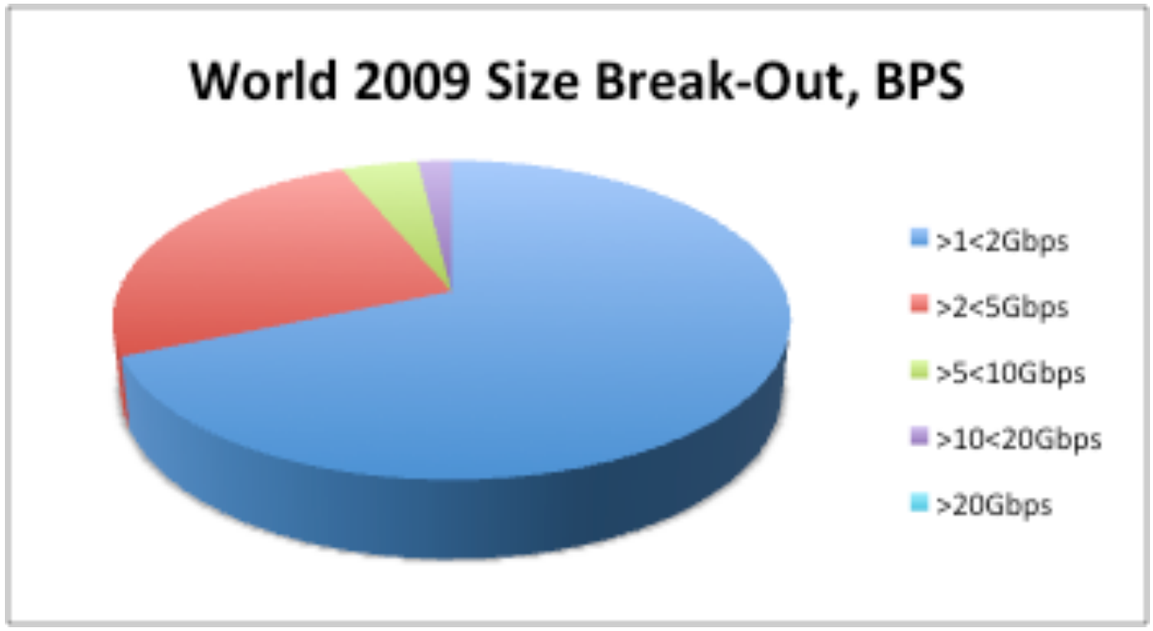


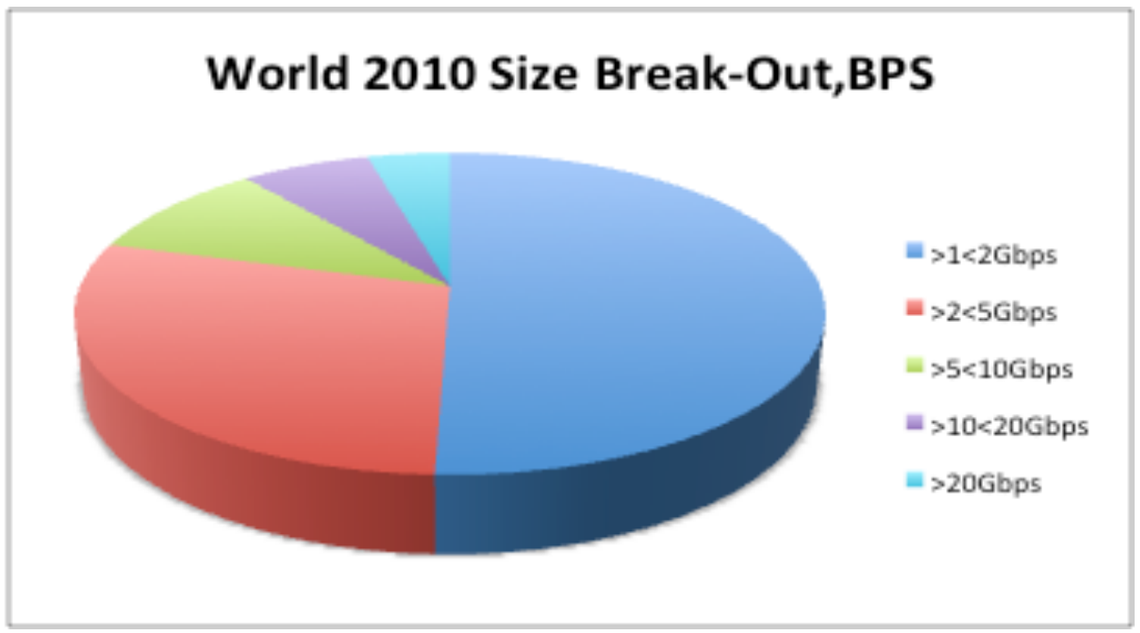


2010 ATLAS Initiative: Internet Trends, World-Wide

Size of Attacks Targeting Port 53 Increase

- Proportion of monitored attacks targeting port 53 stays roughly the same.
- 885% increase in number of attacks over 10Gb/sec





- 247% growth in number of attacks over 10Mpps.
- Multiple attacks monitored at over 40Gb/sec or 50Mpps.

2011 ATLAS Initiative: Internet Trends, World-Wide

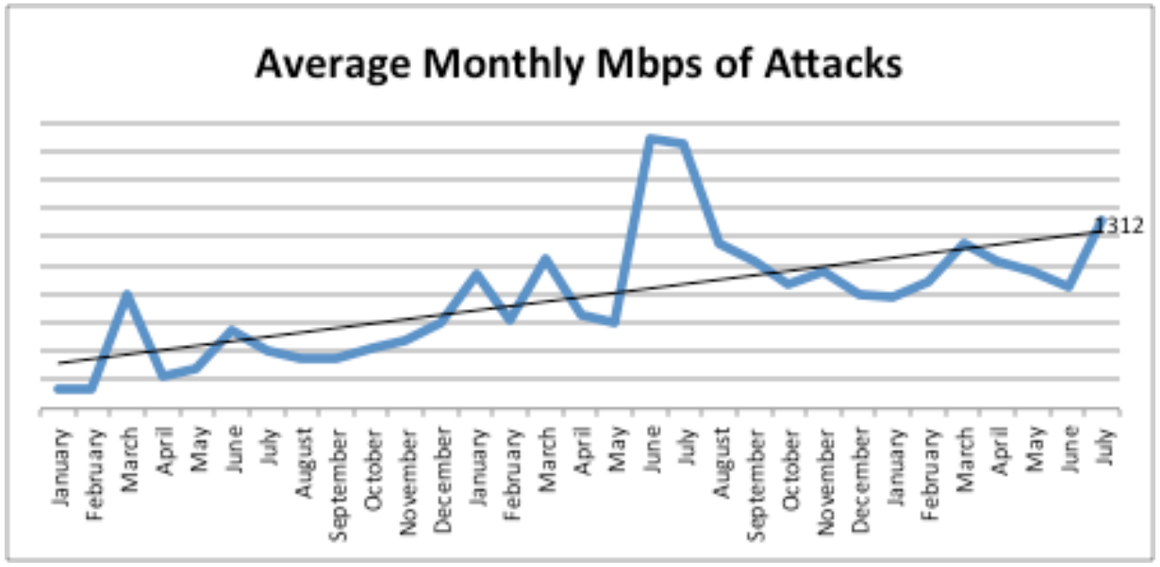
Largest Monitored Attack Sizes Year on Year

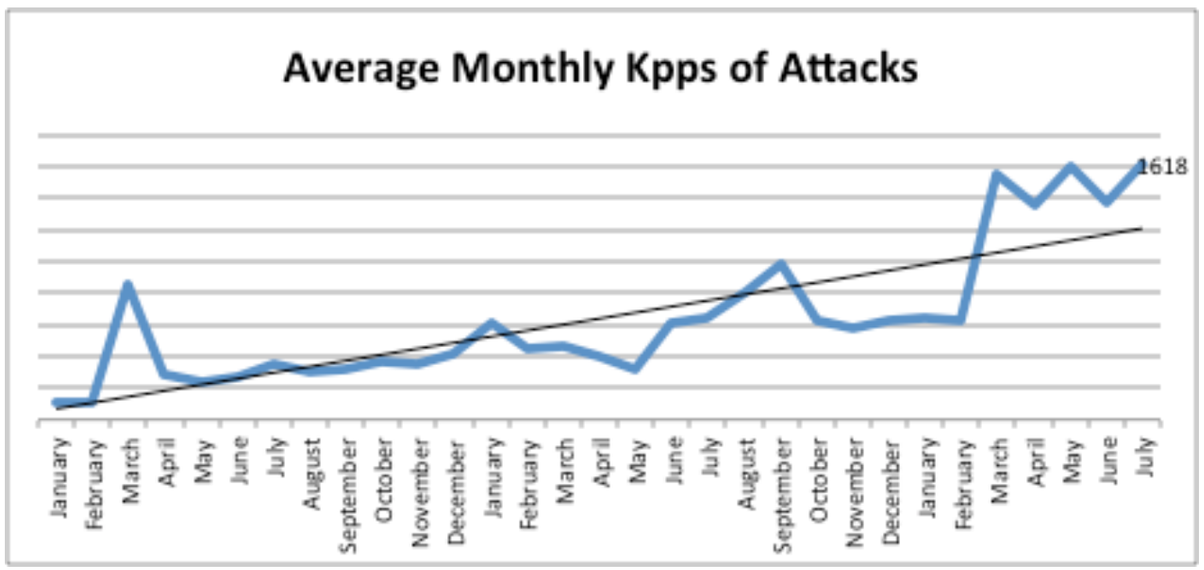
- Largest monitored attack in 2009, BPS:
  - 49.99Gb/sec, Port Range, Taiwan
  - Lasted 1 hour 19 mins.
- Largest monitored attack in 2010, BPS:
  - 66.205Gb/sec, DNS, US
  - Lasted 3 days, 21 hours and 18 minutes.
- Largest monitored attack in 2011 (so far), BPS:
  - 79.27Gb/sec, Port Range, NZ
  - Lasted 2 hours 6 mins
- Largest monitored attack in 2009, PPS :
  - 55.47Mpps, HTTP, US
  - Lasted 17 hours 1 minute
- Largest monitored attack in 2010, PPS:
  - 108.89Mpps, DNS, US
  - Lasted 3 days, 21 hours and 18 minutes
- Largest monitored attack in 2011 (so far), PPS:
  - 71.34Mpps, HTTPS, US
  - Lasted 1 hour 29 minutes

2011 ATLAS Initiative: Internet Trends, World-Wide

Attack Growth trend in Mbps and Kpps

- Average monthly monitored attack size since start of 2009.
- Average attack is 1.31Gbps / 1.62Mpps, July 2011



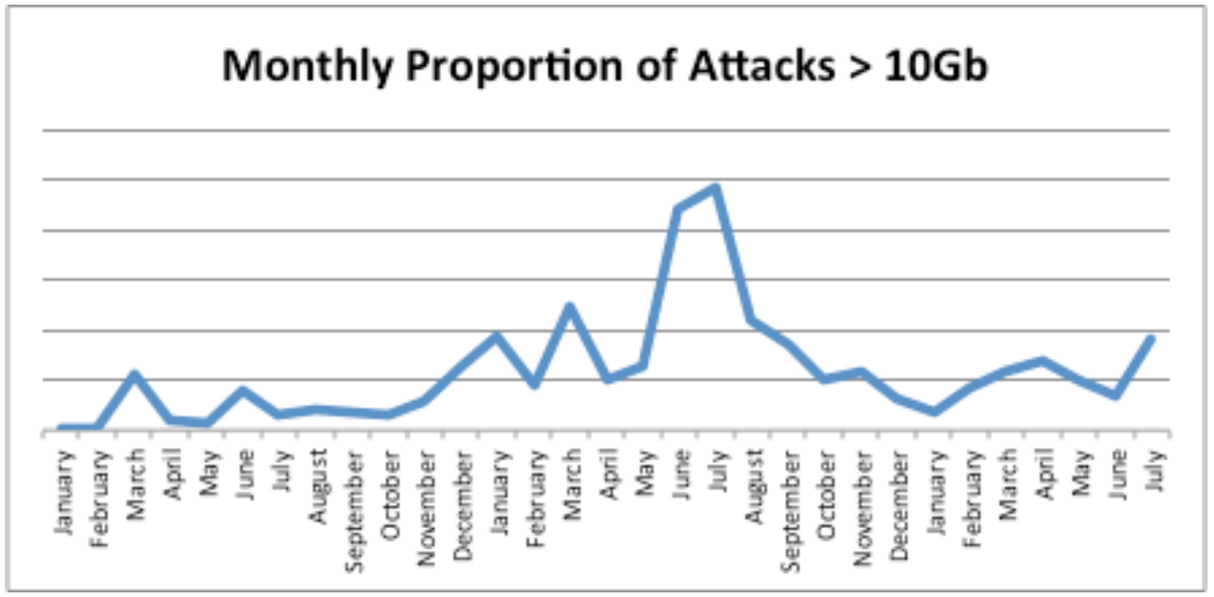


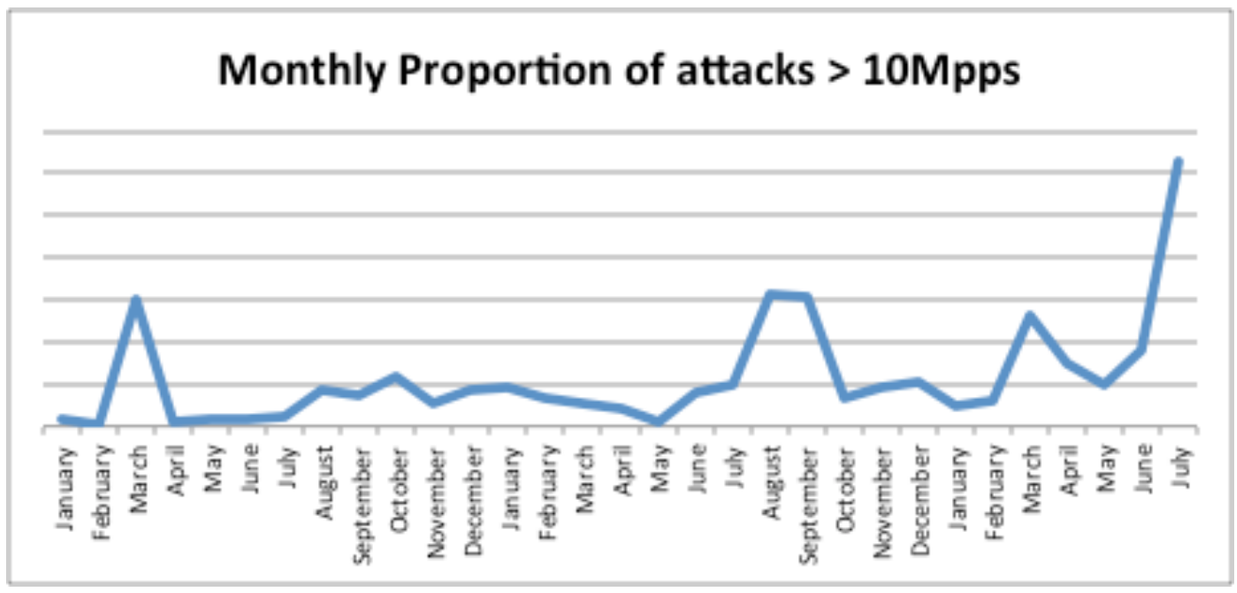
- Average attacks sizes have grown by 40.6% / 165.7% since start of 2010

2011 ATLAS Initiative: Internet Trends, World-Wide

Proportion of Attacks Over 10Gb/sec & 10Mpps

- Proportion of monitored attacks over 10Gb/sec fell at the start of the 2011.
- Growing again now.



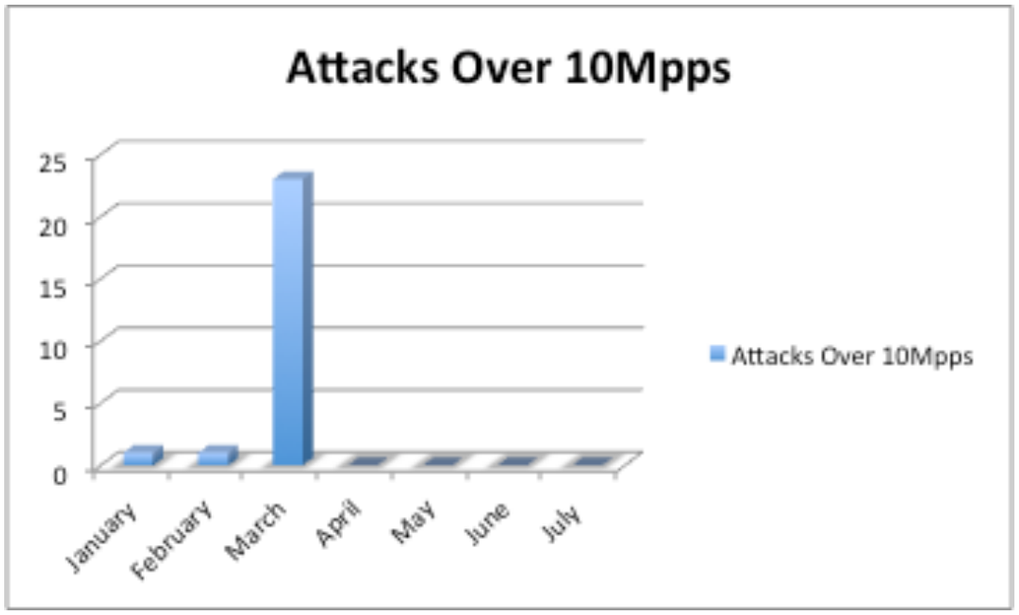


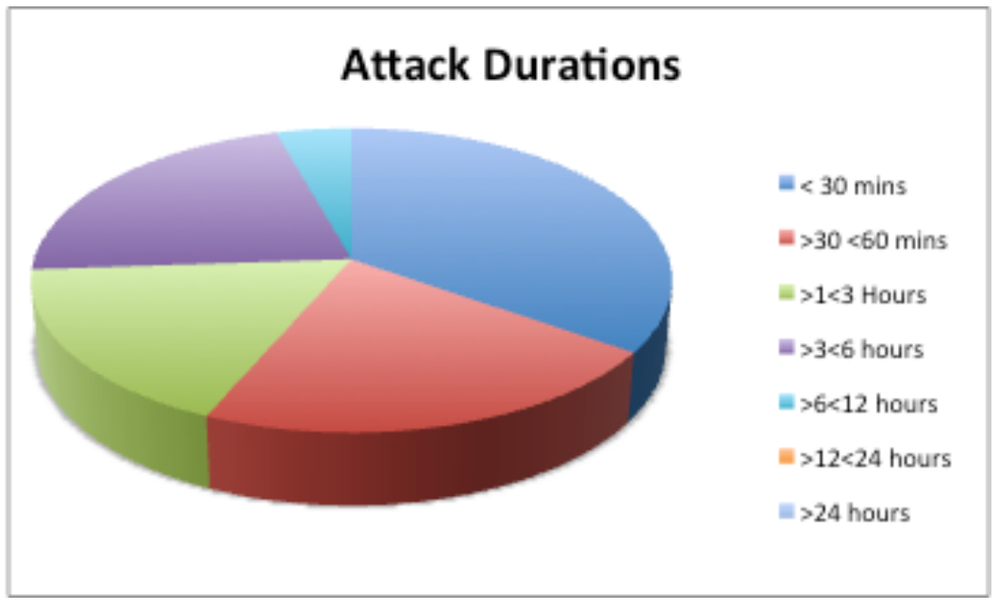
- Spikes in number of attacks over 10Mpps in March and July.
  - March = Belize
  - July = Anonymised

2011 ATLAS Initiative: Internet Trends, World-Wide

Activity Targeting Belize in March 2011

- 23 attacks between 11th an 16th March
- Average size of attack 17.25Mpps
- Largest attack 24.76Mpps
- All targeting port 80
- One specific ISP / Hosting Provider

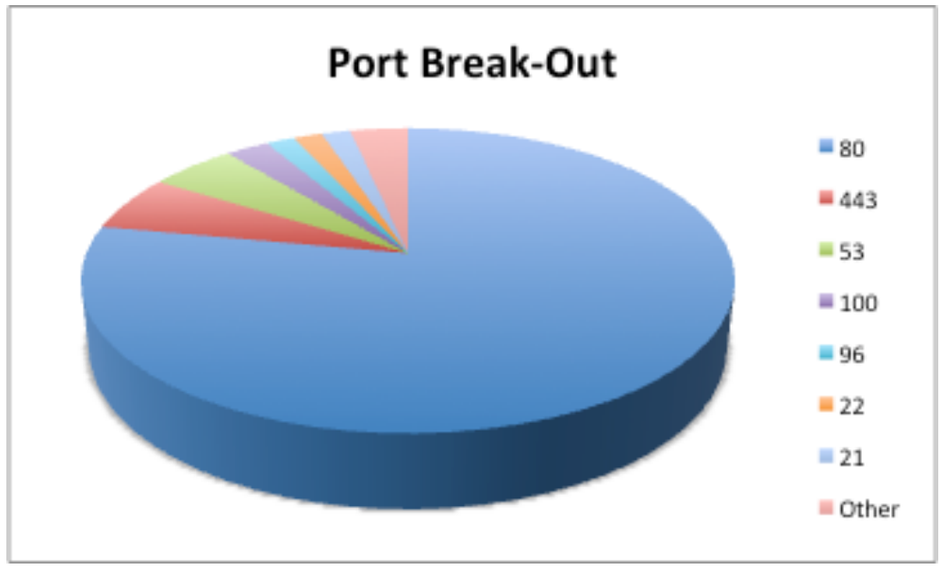


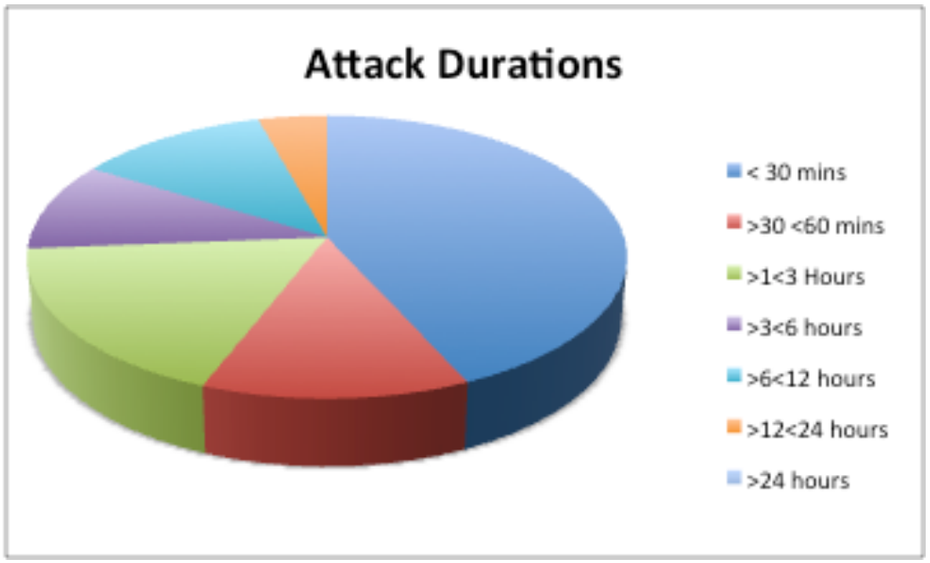


2011 ATLAS Initiative: Internet Trends, World-Wide

Large Number of attacks over 10Mpps in July

- Destination addresses of attacks anonymised
  - No ASN look-up or IP location determination possible.
- 118 attacks over 10Mpps tracked in July.
- Majority of attacks targeting Port 80

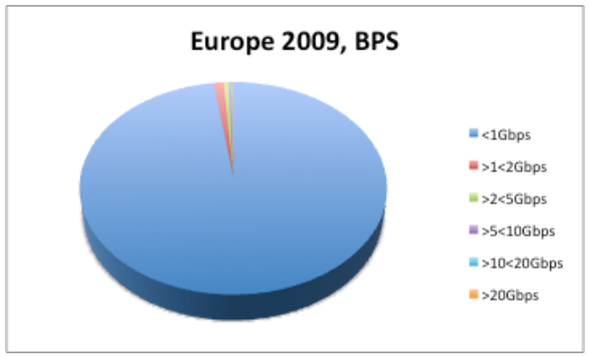


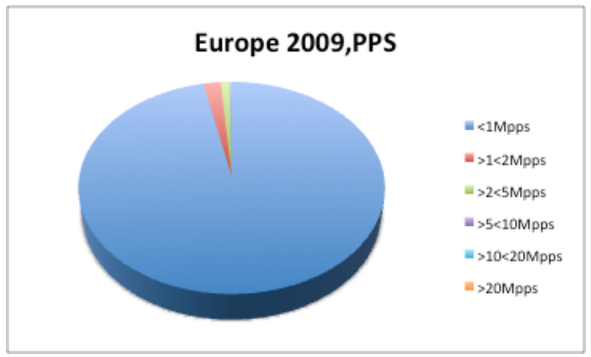


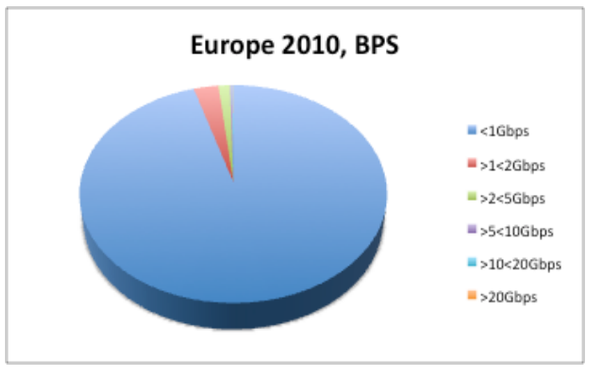
2011 ATLAS Initiative: Internet Trends, Europe

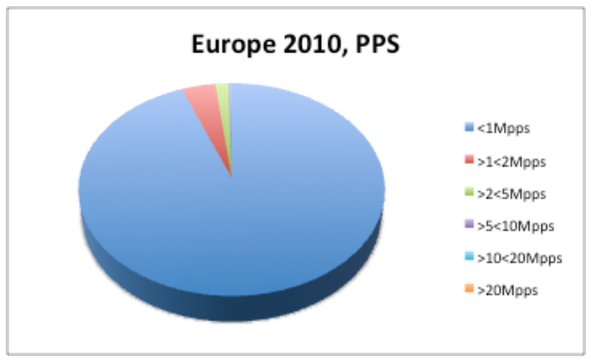
Small Attacks : Europe Focus

- Focus on European Data throughout this talk
  - Countries included : AL, AD, AM, AT, AZ ,BY, BE, BA, BG, CY, HR, CZ, DK, EE, FI, FR, GE, DE, GR, HU, IS,IE, IT, KZ, LI, LV ,LT, LU, MT, MD, MK, MC, ME, NL, NO, PL. PT, RO, RU, SM, RS, SI, SK, ES, CH, SE, TR, UA, UK, GB,VA









- In Europe small attack trend is similar to world-wide:
  - 95.3% less than 1Gb/sec, down from 97.7% 2009
  - 94.1% less than 1Mpps, down from 96.7% 2009
- Average attack sizes:
  - 2009 – 182.72Mbps / 187.79Kpps
  - 2010 – 253.42Mbps / 331.86Kpps

2011 ATLAS Initiative: Internet Trends, Europe

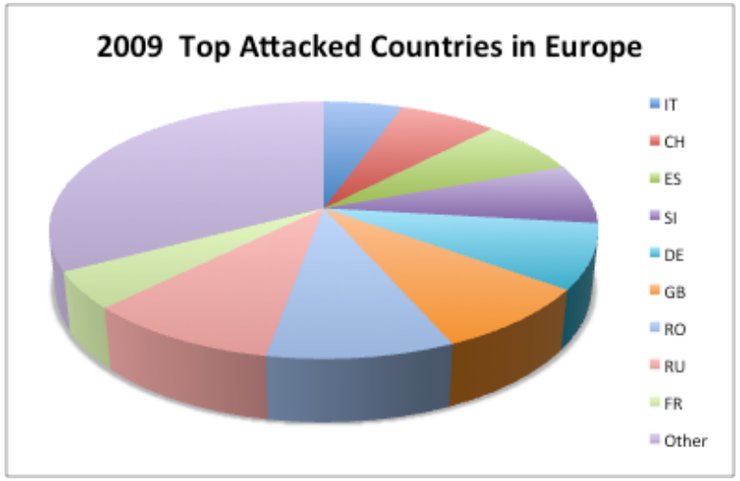
Largest Monitored Attack Sizes Year on Year

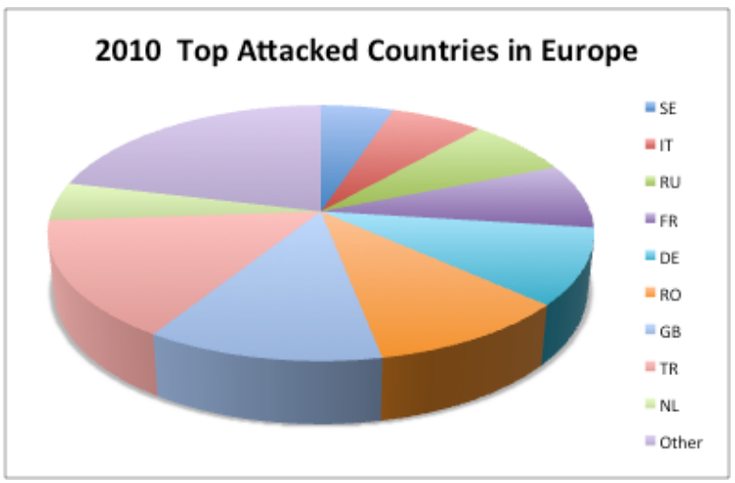
- Largest monitored attack in 2009, BPS:
  - 44.51Gb/sec, Switzerland
  - Lasted 8 hours 10 mins.
- Largest monitored attack in 2010, BPS:
  - 29.89Gb/sec, Russia
  - Lasted 8 hours 7 mins
- Largest monitored attack in 2011 (so far), BPS:
  - 17.78Gb/sec, Romania
  - Lasted 13 hours 8 mins.
- Largest monitored attack in 2009, PPS :
  - 34.12Mpps, Belgium
  - Lasted 7 hours 2 mins
- Largest monitored attack in 2010, PPS:
  - 39.25Mpps, Spain
  - Lasted 28 mins
- Largest monitored attack in 2011 (so far), PPS:
  - 33.75Mpps, Russia
  - Lasted 21 hours 2 mins

2010 ATLAS Initiative: Internet Trends, Europe

Top Destination Countries by Monitored Attacks

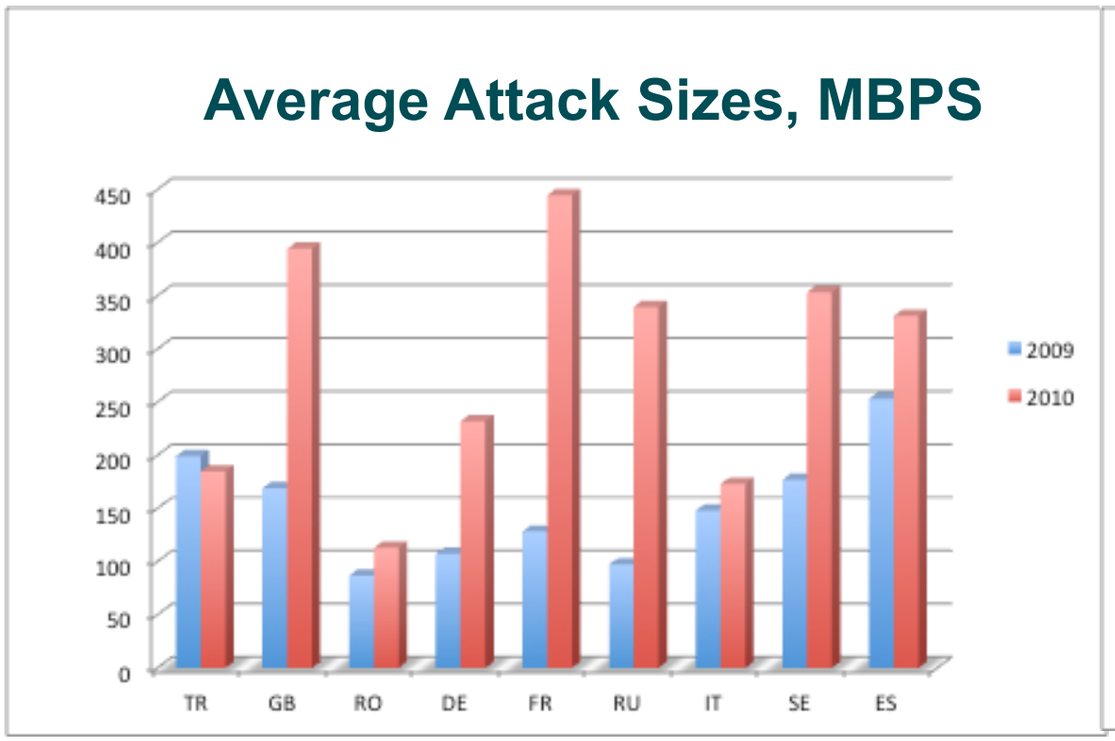
Country	Rank 2009	Rank 2010	Change
Turkey	-	1	New Entry
Great Britain	3	2	↑
Romania	2	3	↓
Germany	4	4	=
France	9	5	↑
Russia	1	6	↓
Italy	8	7	↑

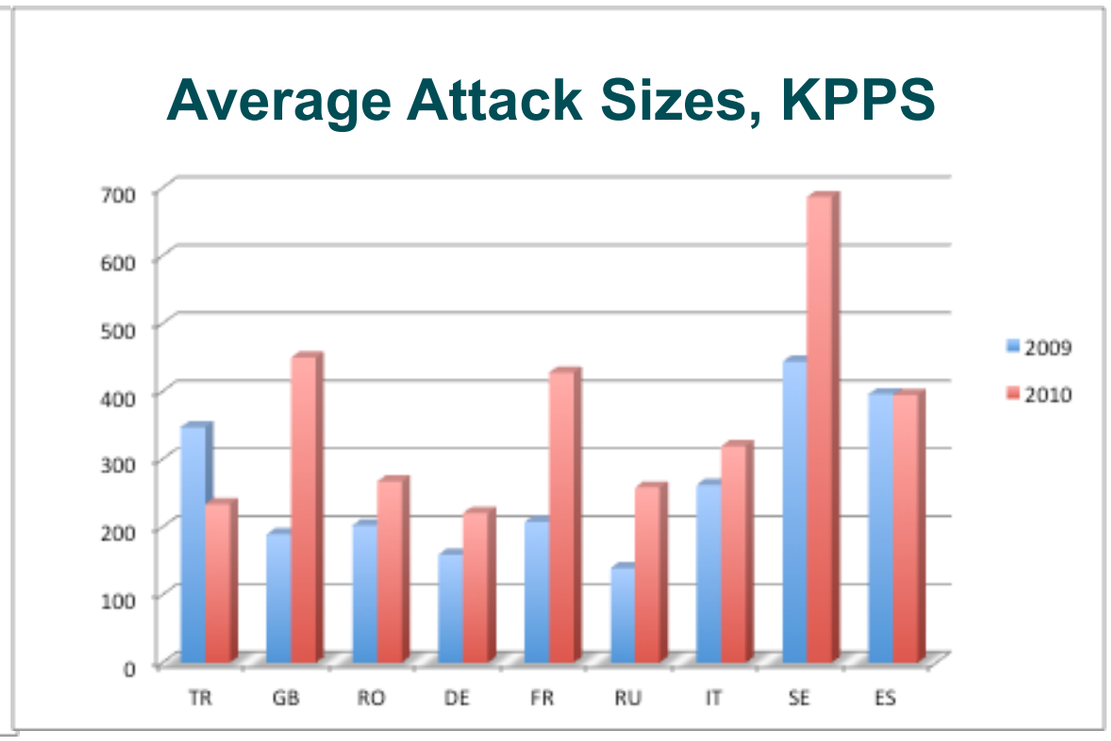




2010 ATLAS Initiative: Internet Trends, Europe

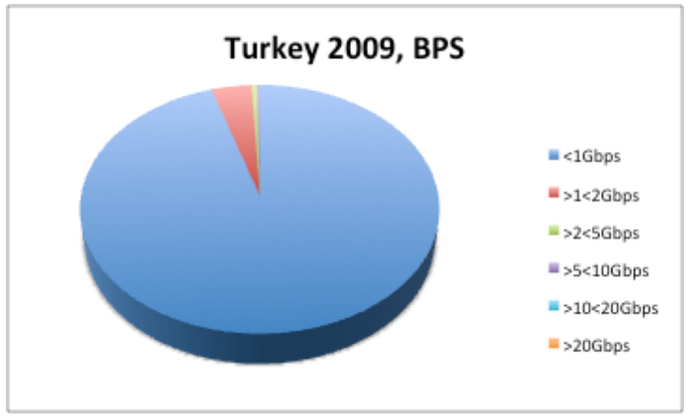
Average Attack Sizes Grow for Most Targeted Countries

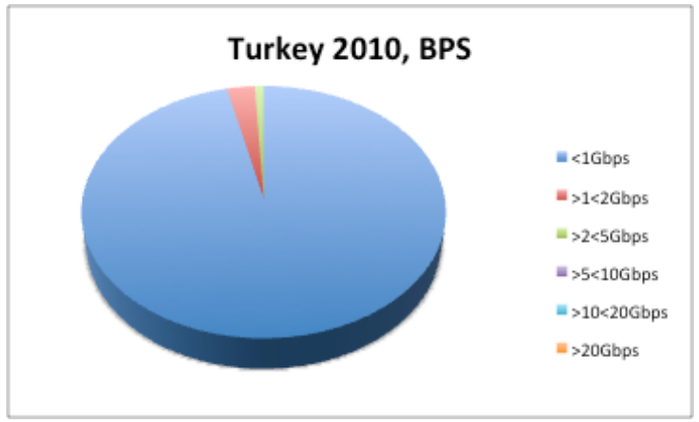


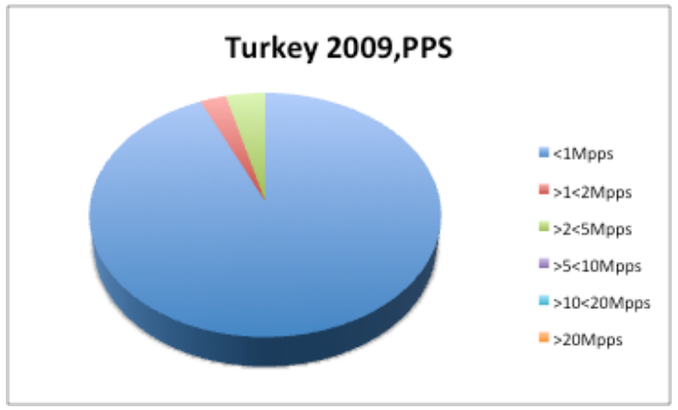


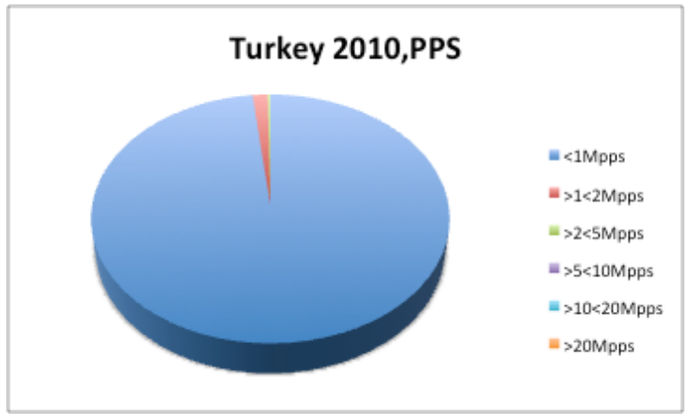
2010 ATLAS Initiative: Internet Trends, TR (#1)

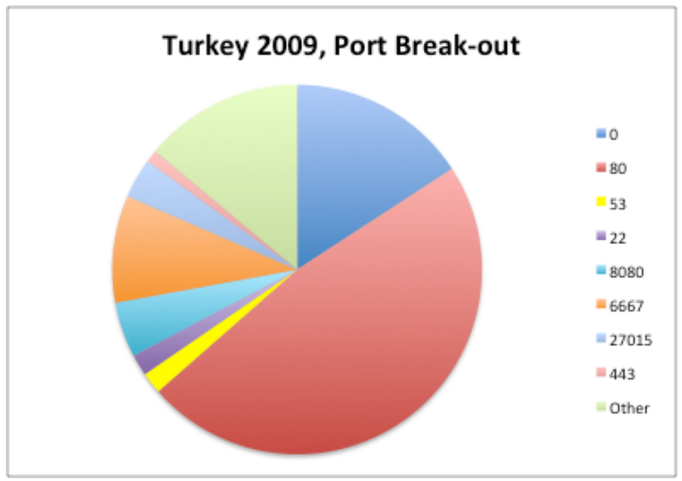
- Slight increase in proportion of attacks less than 1Gb/sec or 1Mpps.
  - 96.4.7% less than 1Gb/sec (up from 95.2% in 2009)
  - 98.2% less than 1Mpps (up from 96.4% in 2009)
  - Massive increase in number of reported events from 2009.
- Port 80 dominates as most prevalent attack target
  - 47.7% in 2009, 53.7% 2010
- Proportion of attacks targeting port 53 very low.
  - 1.9% vs approx 12% world-wide

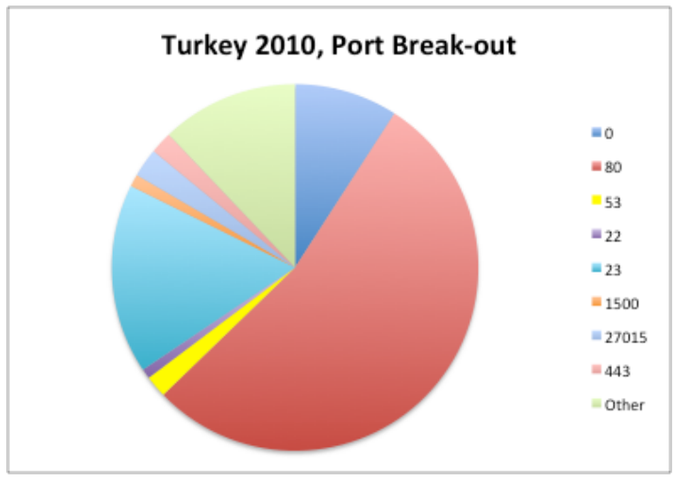












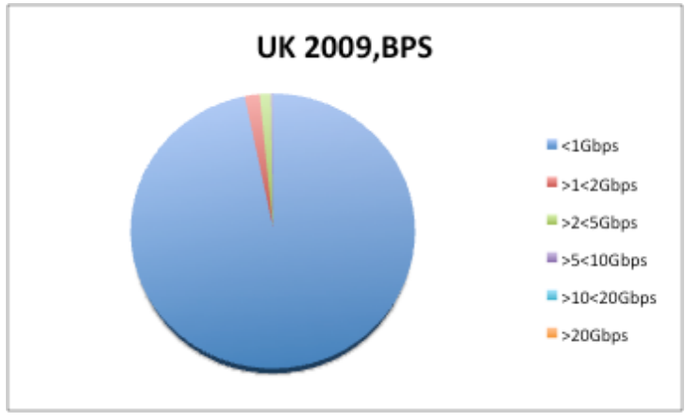
2010 ATLAS Initiative: Internet Trends, TR (#1)

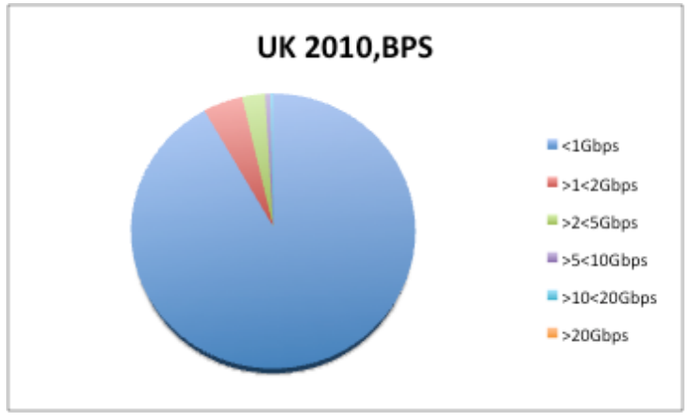
Largest Attacks Seen in TR 2009, 2010, 2011 (so far)

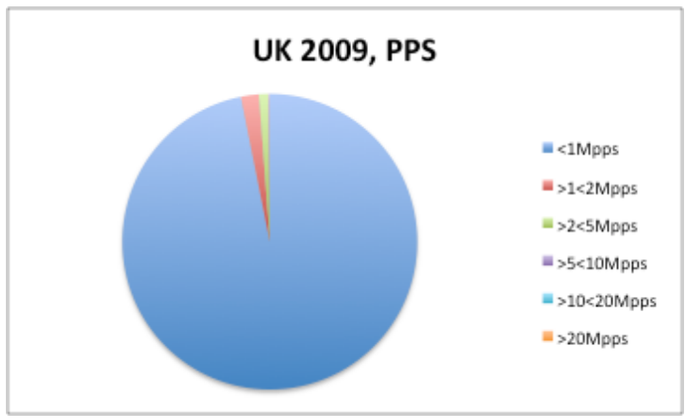
- Largest monitored attack in 2009, BPS:
  - 5.51Gb/sec – 4.36Mpps
  - Lasted 10 mins.
- Largest monitored attack in 2010, BPS:
  - 4.4Gb/sec – 584.75Kpps
  - Lasted 16 mins.
- Largest monitored attack in 2011 (so far), BPS:
  - 13.83Gb/sec – 22.16Mpps
  - Port 22
  - Lasted 10 mis.
- Largest monitored attack in 2009, PPS :
  - 4.95Mpps – 1.9 Gb/sec
  - Port 80
  - Lasted 11 hours 31 mins
- Largest monitored attack in 2010, PPS:
  - 4.08Mpps – 1.44Gb/sec
  - Port 80
  - Lasted 12 hours 17 mins.
- Largest monitored attack in 2011 (so far), PPS:
  - 22.16Mpps – 13.83Gb/sec
  - Port 22
  - Lasted 10 mins

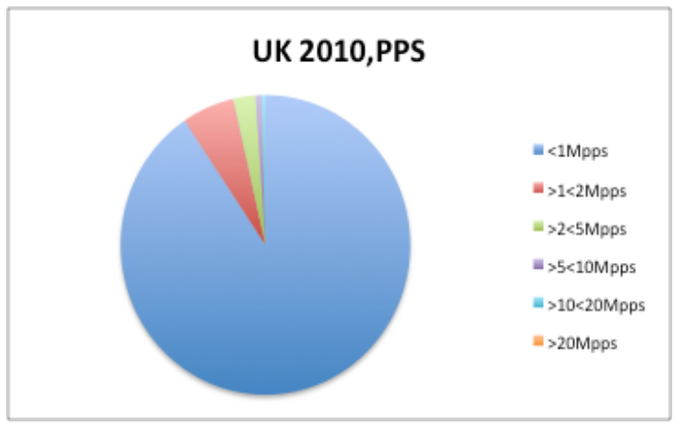
2010 ATLAS Initiative: Internet Trends, GB (#2)

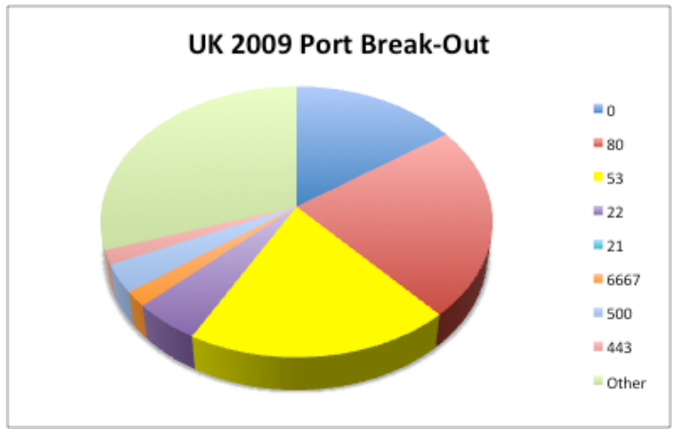
- Similar trend in proportion of attacks less than 1Gb/sec or 1Mpps to world-wide data.
  - 91.7% less than 1Gb/sec (down from 96.7% in 2009)
  - 90.6% less than 1Mpps (down from 96.9% in 2009)
- Proportion of attacks targeting ports 80 and 53 staid approx the same.
- All attacks over 10Gb/sec in 2010 targeting port 53.

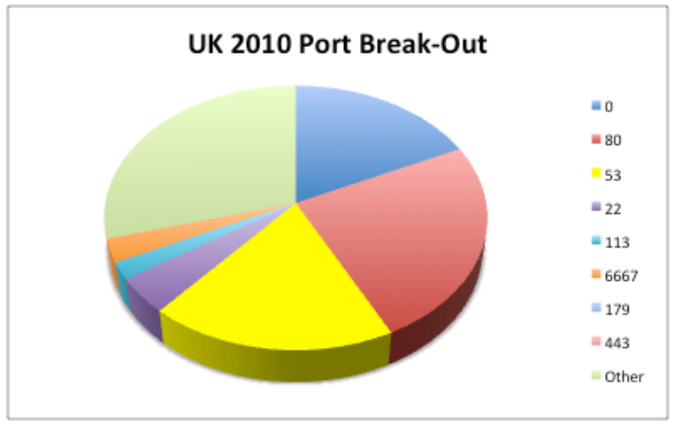












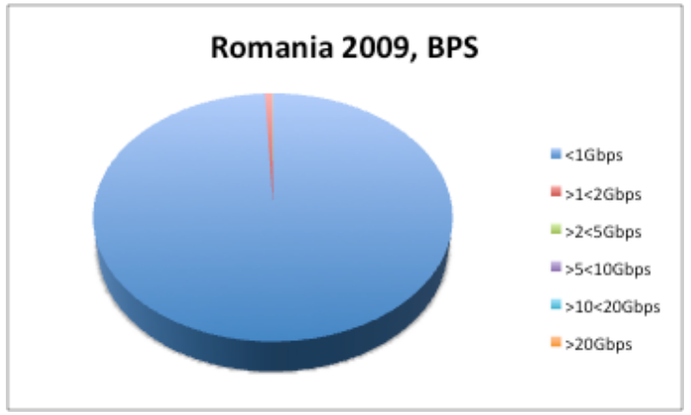
2010 ATLAS Initiative: Internet Trends, GB (#2)

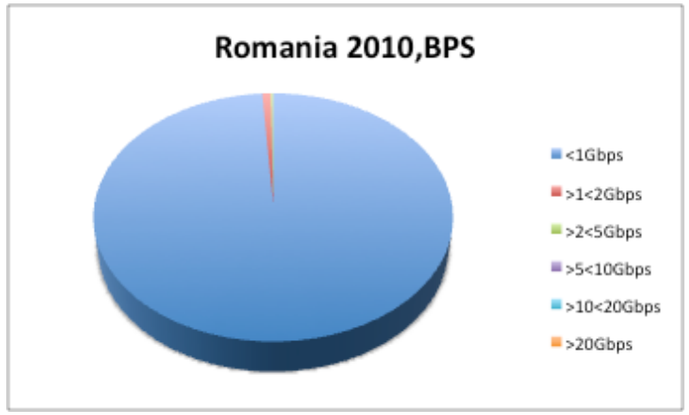
Largest Attacks Seen in GB 2009, 2010, 2011 (so far)

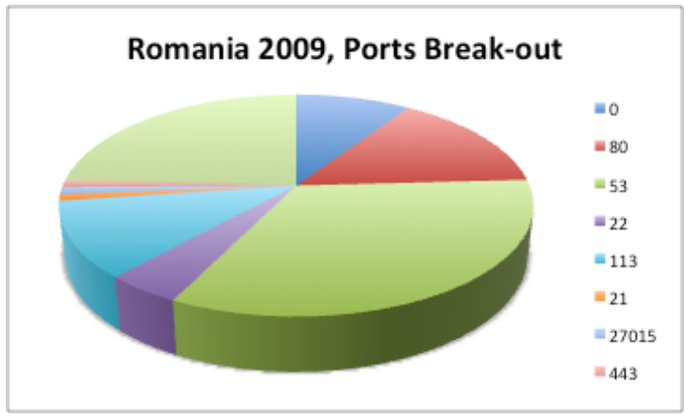
- Largest monitored attack in 2009, BPS:
  - 6.29Gb/sec – 555Kpps
  - Port 60345
  - Lasted 5 hours 23 mins.
- Largest monitored attack in 2010, BPS:
  - 15.89Gb/sec - 3.12Mpps
  - Port 53
  - Lasted 2 hours 4 mins.
- Largest monitored attack in 2011 (so far), BPS:
  - 5.89Gb/sec – 1.05Mpps
  - Port 25345
  - Lasted 19 mins
- Largest monitored attack in 2009, PPS :
  - 5.76Mpps - 2.21 Gb/sec
  - Port 22
  - Lasted 2 hours 11 mins
- Largest monitored attack in 2010, PPS:
  - 14.953Mpps - 7.18Gb/sec
  - Port 6102
  - Lasted 6 mins.
- Largest monitored attack in 2011 (so far), PPS:
  - 14.57Mpps – 4.43Gb/sec
  - Port 21
  - Lasted 44 mins

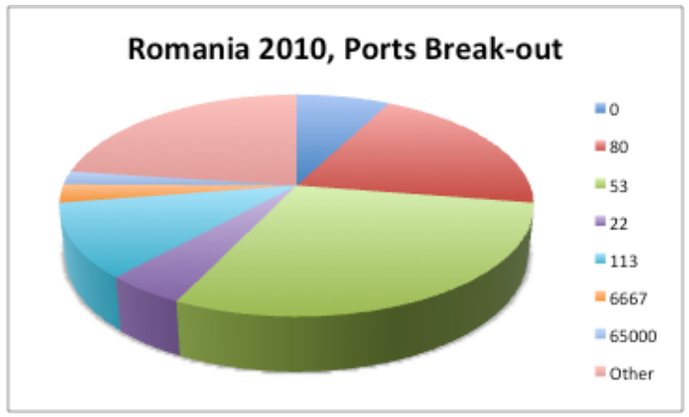
2010 ATLAS Initiative: Internet Trends, RO (#3)

- Not much changes in proportion of attacks less than 1Gb/sec or 1Mpps.
  - 98.9% less than 1Gb/sec (down from 99.2% in 2009)
  - 95.5% less than 1Mpps (down from 97.5% in 2009)
- Proportion of attacks targeting ports 80 grew from 14.8% to 19.8%.
- Proportion of attacks targeting port 53 is unusually high
  - 2009 = 33.1%
  - 2010 = 29.8%
  - Globally 2010 = 12.2%









2010 ATLAS Initiative: Internet Trends, RO (#3)

Largest Attacks Seen in RO 2009, 2010, 2011 (so far)

- Largest monitored attack in 2009, BPS:
  - 2.57Gb/sec – 6.7Mpps
  - Port 80
  - Lasted 13 mins.
- Largest monitored attack in 2010, BPS:
  - 2.76Gb/sec – 4.42Mpps
  - Port 22
  - Lasted 1 hours 2 mins.
- Largest monitored attack in 2011 (so far), BPS:
  - 17.78Gb/sec – 2Mpps
  - Lasted 13 hours 8 mins.
- Largest monitored attack in 2009, PPS :
  - 2.57Gb/sec – 6.7Mpps
  - Port 80
  - Lasted 13 mins.
- Largest monitored attack in 2010, PPS:
  - 5.94Mpps – 2.04Gb/sec
  - Port 53
  - Lasted 2 hours 8 mins.
- Largest monitored attack in 2011 (so far), PPS:
  - 6.4Mpps – 2.2Gb/sec
  - Lasted 10 mins

Questions?