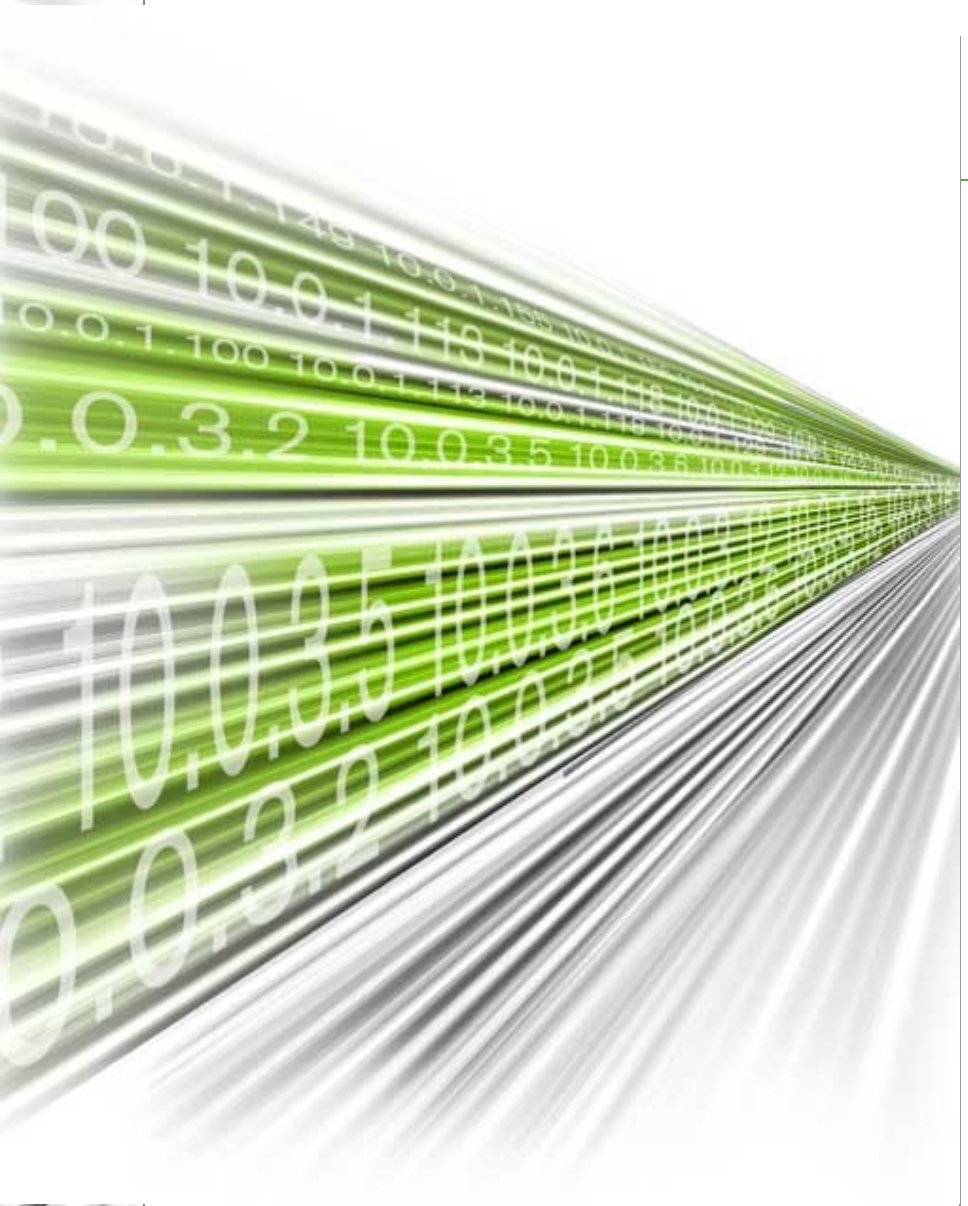


ATLAS Initiative : Update 2010 – 2011 Q2 DDoS Analysis

Darren Anstee
Solutions Architect

Introduction

- Darren Anstee, EMEA Solutions Architect.
- 17+ years of experience in Networking and Security.
- 8+ years at Arbor Network

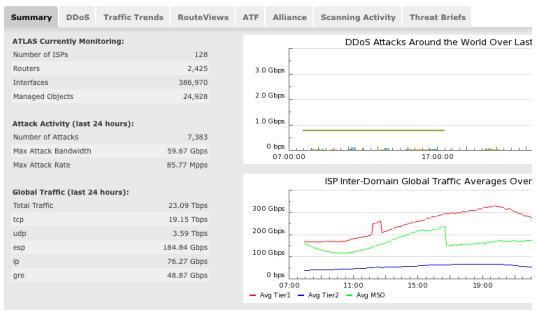
- 300+ employees in 20+ countries
- 300+ customers
  - 90%+ of Tier1 providers,
  - 60%+ of Tier2 providers, 11 of 13 of NA MSOs.
- Privileged relationships with majority of world's ISPs
- ATLAS / ASERT thought leadership.

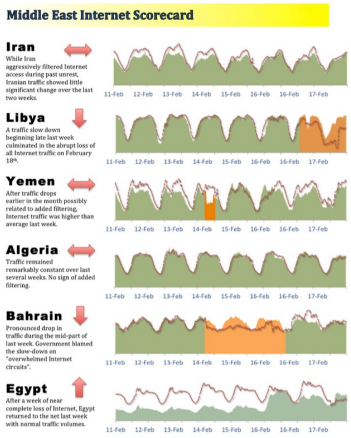
ARBOR® NETWORKS
How networks grow™

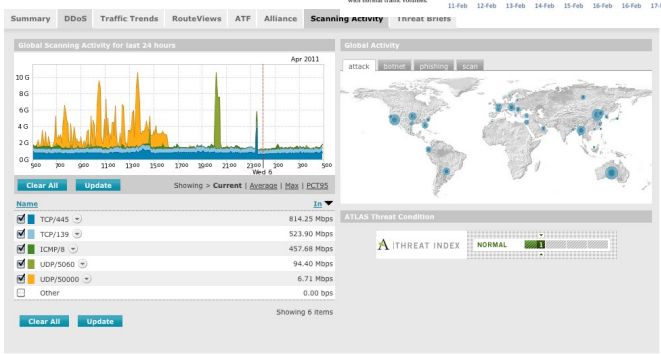
ARBOR® NETWORKS

The Arbor ATLAS Initiative

- **What is it?**
  - **A**ctive **T**hreat **L**evel **A**nalysis **S**ystem
  - **A set of tools to model internet traffic patterns and Internet threat evolution**
- **How is it used?**
  - **Within Arbor Products**
  - **Atlas.arbor.net site / Blog**
  - **Various Presentations**
  - **Trends in Internet Traffic Patterns – NANOG 47 / MENOG**
  - **Botnet, DDoS and Ground Truth – NANOG 50**
  - **Broader Security Community**
- **What is it for?**
  - **Broaden our understanding of the Internet**







The Arbor ATLAS Initiative: Internet Trends

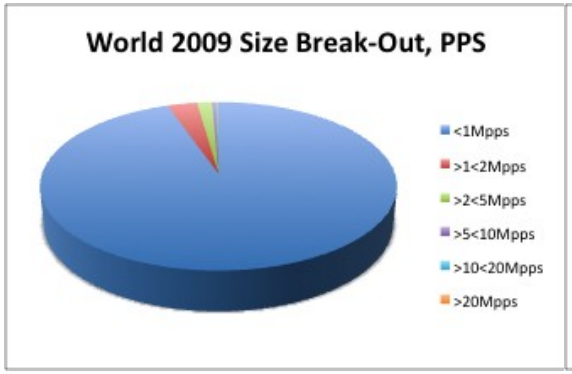
- **180+ ISPs sharing real-time data - > ATLAS Internet Trends**
  - Automated hourly export of XML file to Arbor server (HTTPS)
  - File is anonymous, only tagged with
  - User Specified Region e.g. Europe
  - Provider Type (self categorized) e.g. Tier 1
  - Source / Destination addresses from within 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

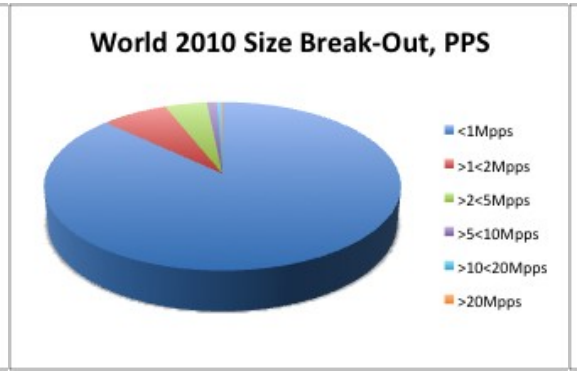
ARBOR NETWORKS

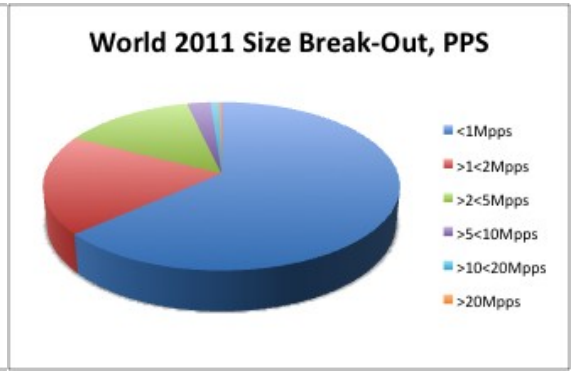
2011 ATLAS Initiative : Anonymous Stats

Small Attacks Continue to Make Up the Majority

- As in 2010 most monitored attacks still small in 2011 :
  - 78.5% less than 1Gb/sec (down from 93% in 2009 and 79% in 2010)
  - 63.5% less than 1Mpps (down from 94% in 2009 and 87% in 2010)
- Average size of attacks,
  - Less than 1Gb/sec:
  - 2010 is 197.41Mbps / 307.72Kpps
  - 2011 is 332.1Mbps / 739.2Kpps
  - Less than 1Mpps:
  - 2010 is 558.96Mbps / 228.139Kpps
  - 2011 is 599.2Mbps / 335.7Kpps



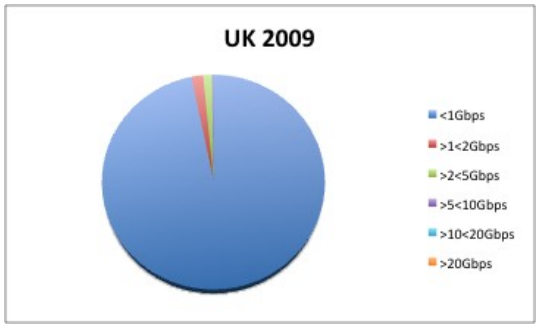


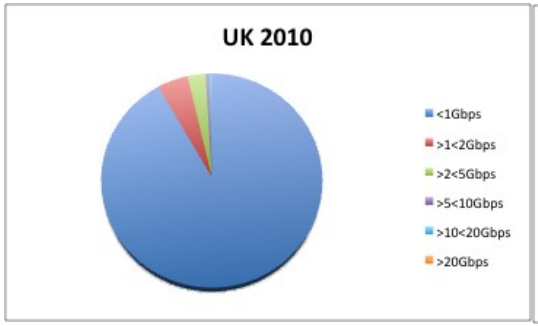


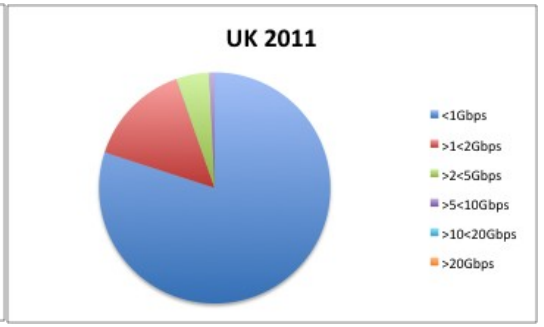
2011 ATLAS Initiative : Anonymous Stats

Small Attacks : UK Focus

- Not a huge amount of data for UK specific attacks:
  - Historically, lack of participation in ATLAS Internet Trends
  - Anonymisation of attack dst addresses, in some cases, makes IP impossible.
- In the UK small attack trend is similar to world-wide:
  - 80% less than 1Gb/sec (down from 96.7% 2009, and 91.7% 2010)
  - 66.9% less than 1Mpps (down from 96.8% 2009, and 90.5% 2010)



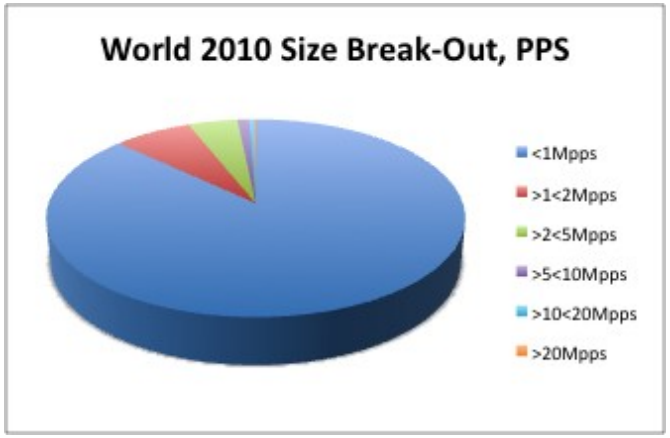




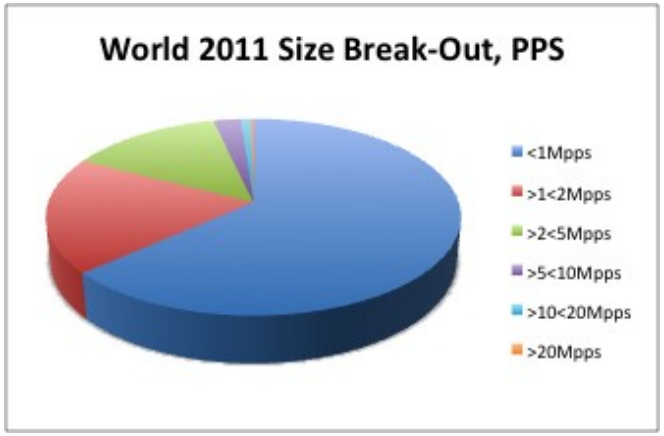
2011 ATLAS Initiative : Anonymous Stats

Proportion of attacks over 10Mpps on the rise!

- Proportion of monitored attacks over 10Gb/sec up 470% from 2009 -> 2010.
- Proportion of monitored attacks over 10Gb/sec has dropped by 48% so far in 2011, compared to 2010.



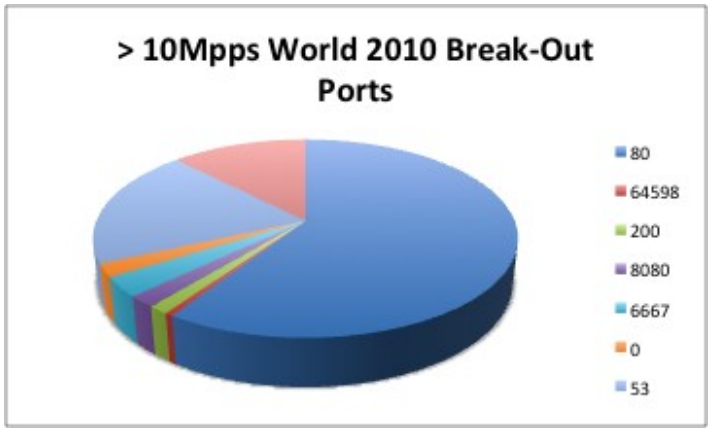
- Proportion of monitored attacks over 10Mpps has increased by 98.4% so far in 2011, compared to 2010.

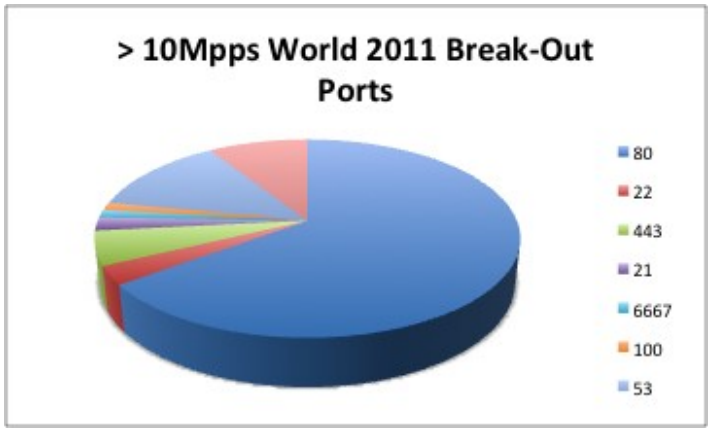


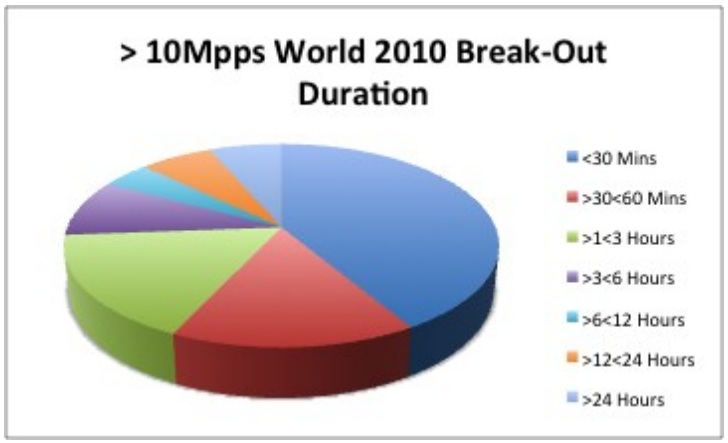
ARBOR NETWORKS

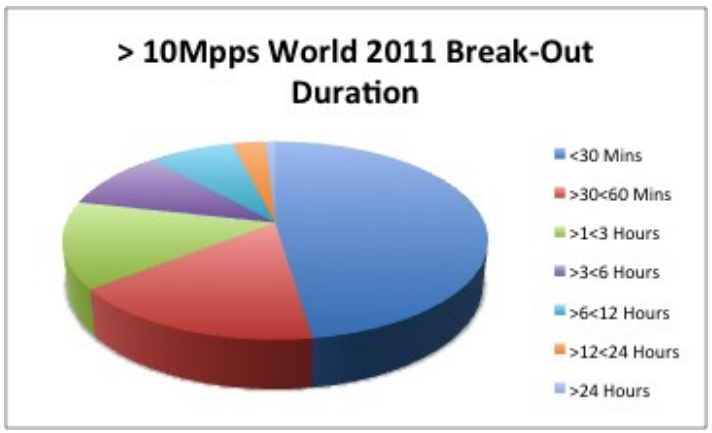
2011 ATLAS Initiative : Anonymous Stats

Changes in Attacks Over 10Mpps









2011 ATLAS Initiative : Anonymous Stats

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:
  - 65.761Gb/sec, 22616, Unknown
  - Lasted 42 minutes.
- 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

ARBOR NETWORKS

2011 ATLAS Initiative : UK

Largest Attacks Seen in UK 2009, 2010, 2011

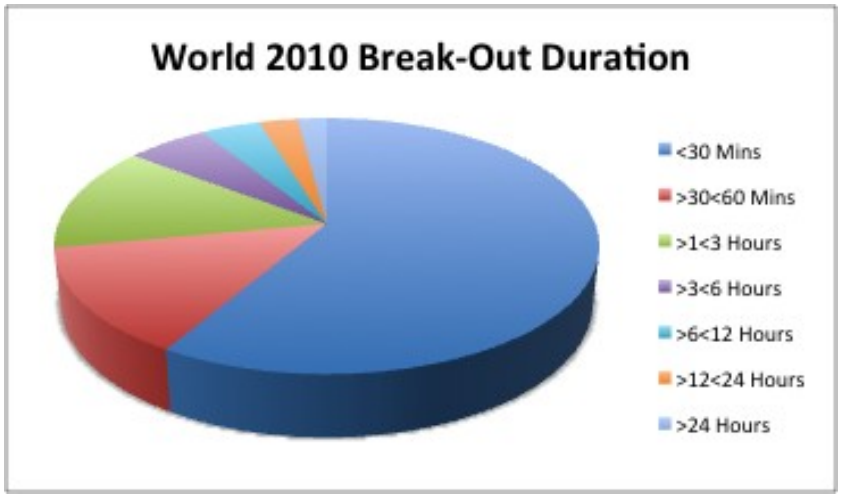
- Largest monitored attack in 2009, BPS:
  - 6.29Gb/sec – 555Kpps
  - Port 60345
  - Lasted 5 hours 23 mins.
- Largest monitored attack in 2010, BPS:
  - 15.89Gb/sec - 3.12Mpps
  - Port 53
  - Lasted 2 hours 4 mins.
- Largest monitored attack in 2011 (so far), BPS:
  - 5.89Gb/sec – 1.05Mpps
  - Port 25345
  - Lasted 19 mis.
- 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

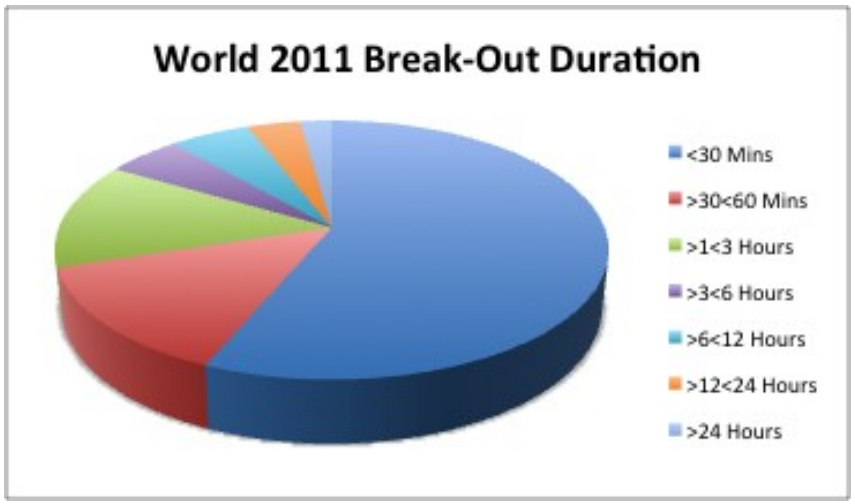
ARBOR NETWORKS

2011 ATLAS Initiative : Anonymous Stats

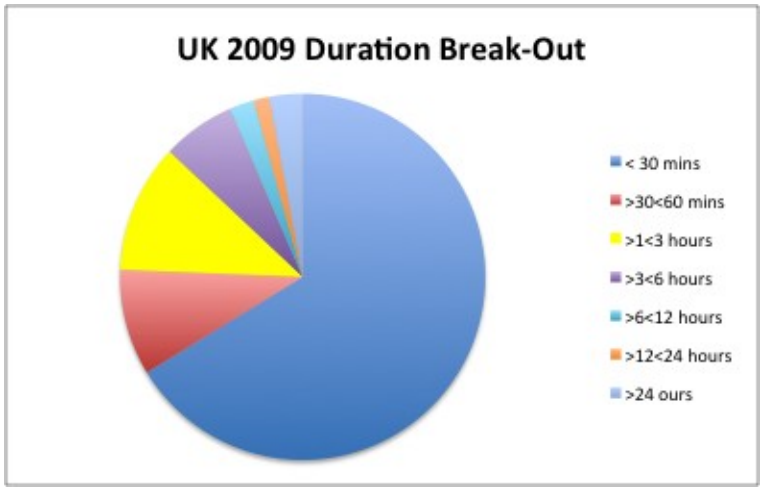
Attack Duration Mix Almost Constant

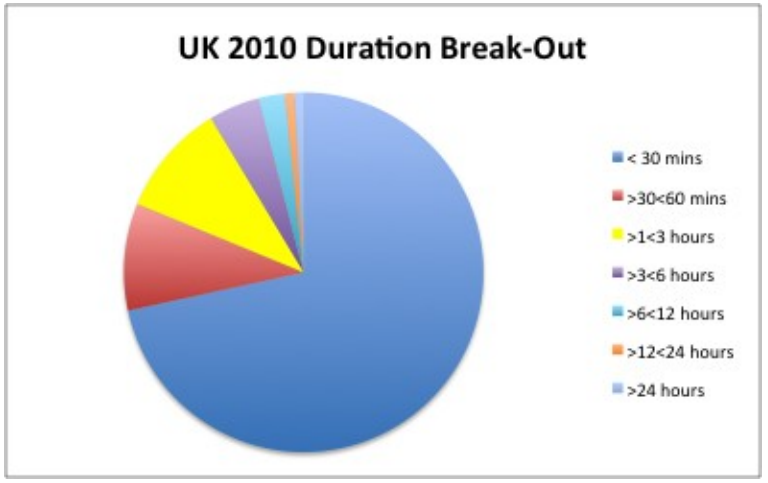
- Majority of attacks short-lived.
- Approx 70% less than 1 hour
- Number of attacks lasting longer than 12 hours up from 4.8% to 5.9%.

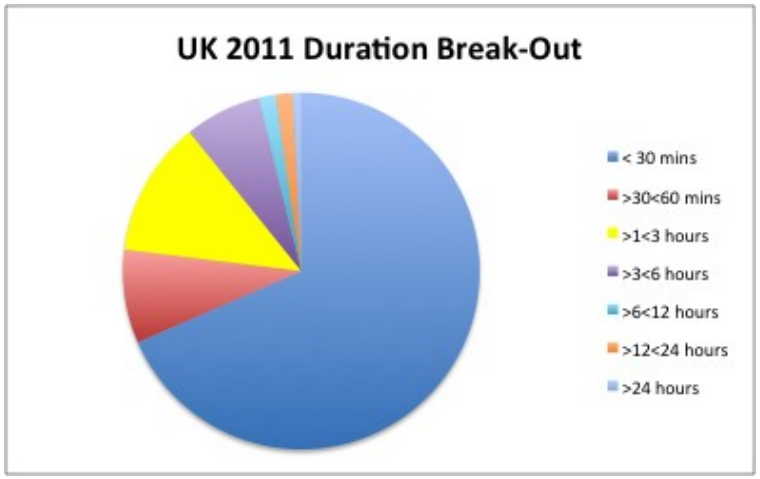




2011 ATLAS Initiative : Details, UK





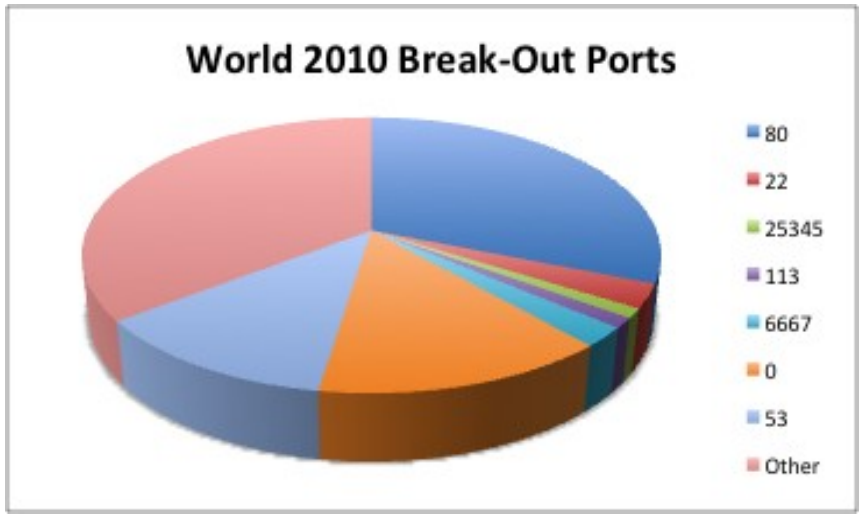


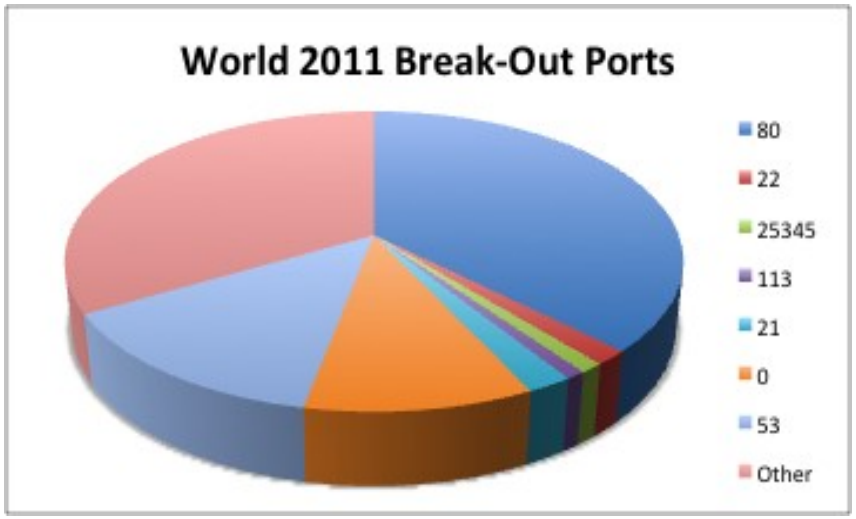
- Not much change in attack duration mix for the UK year on year.
- Roughly 77% of attacks last less than 60 minutes.

2011 ATLAS Initiative : Anonymous Stats

Proportion of Attacks Targeting Port 80 Increases

- In 2009, 19.6% of monitored attacks targeted port 80.
- In 2010 this had increased to 31%, and so far in 2011 we are at 37.3%.
- Attacks targeting fewer ports
  - 80 and 53 most prevalent.
- 75% drop in proportion of attacks over 10Gb/sec (port 80), from 2010 – still 47% up from 2009.



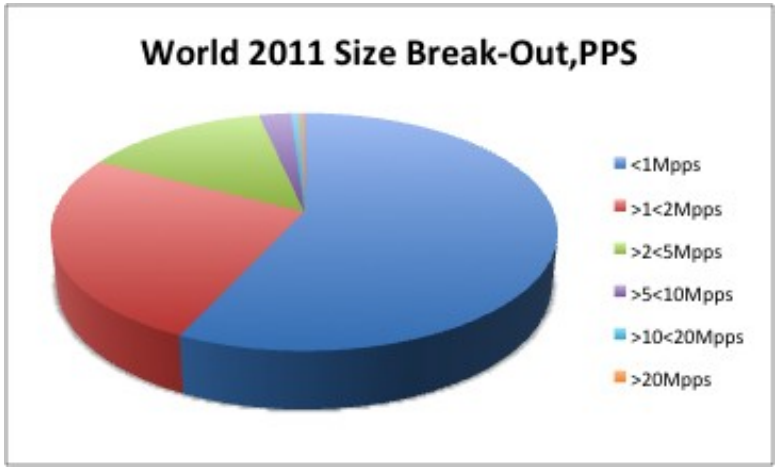


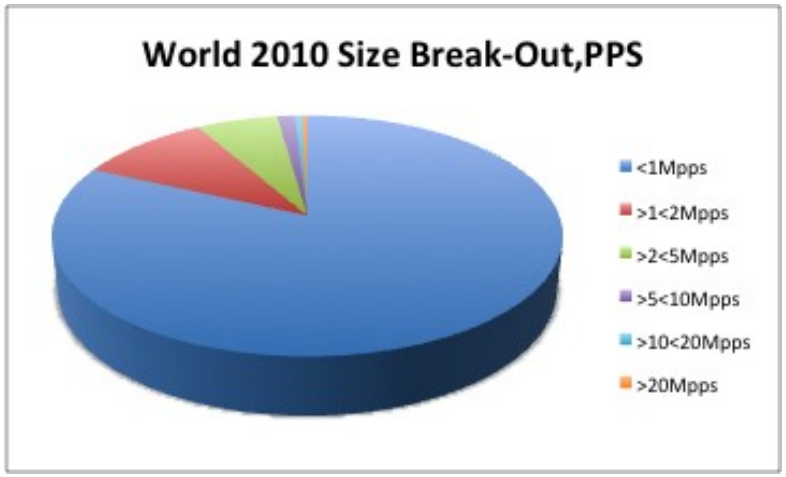
ARBOR NETWORKS

2011 ATLAS Initiative : Anonymous Stats

Average size of Attacks Targeting Port 53 Increase

- Proportion of monitored attacks targeting port 53 stays roughly the same.
- 58.9% drop in proportion of attacks over 10Mpps from 2010, still up 42.9% from 2009.

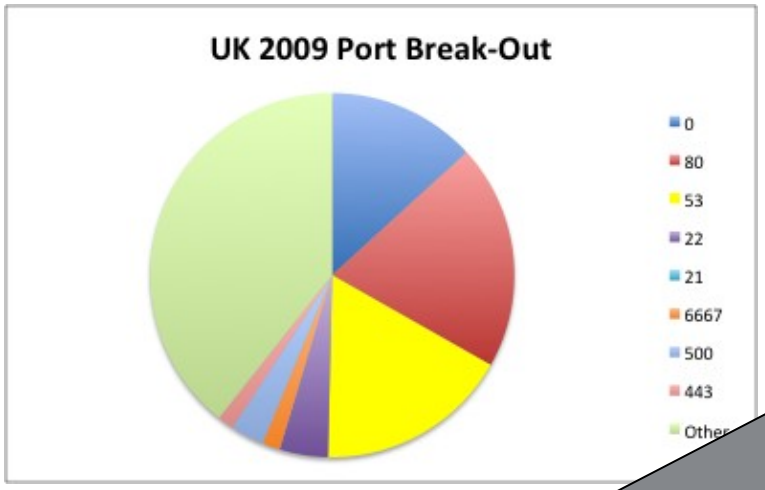


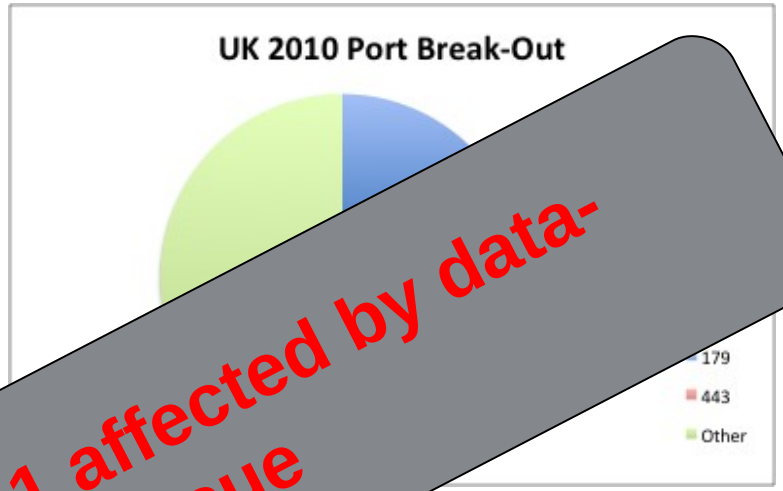


- Overall, average attack sizes shifting up.
- Largest monitored attacks so far this year:
  - 46.5Mpps
  - 21.36Gbps

ARBOR NETWORKS

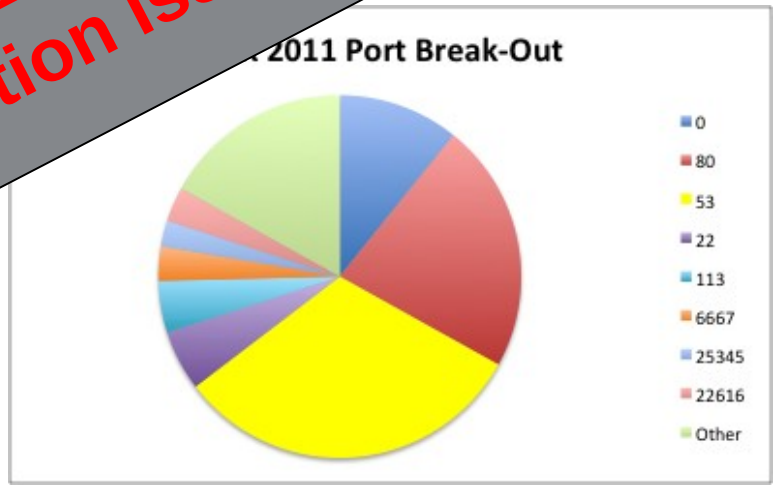
2011 ATLAS Initiative : Details, UK





- Proportion of of at
  targeting p
  15.9%
- P

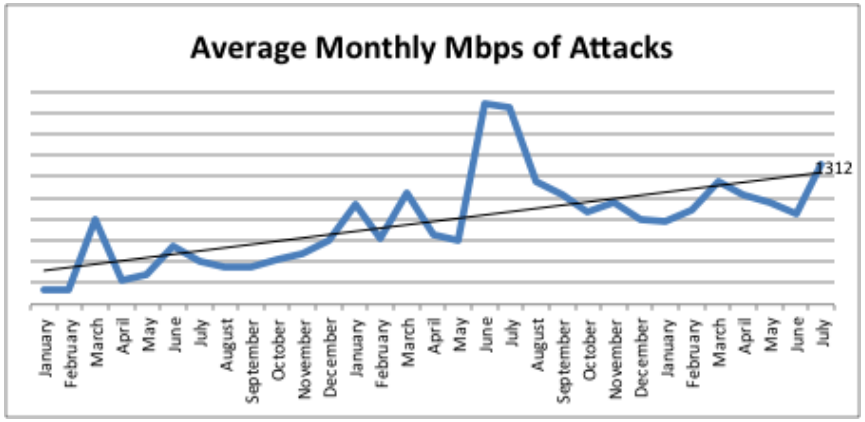
UK Data for 1H 2011 affected by data-collection issue

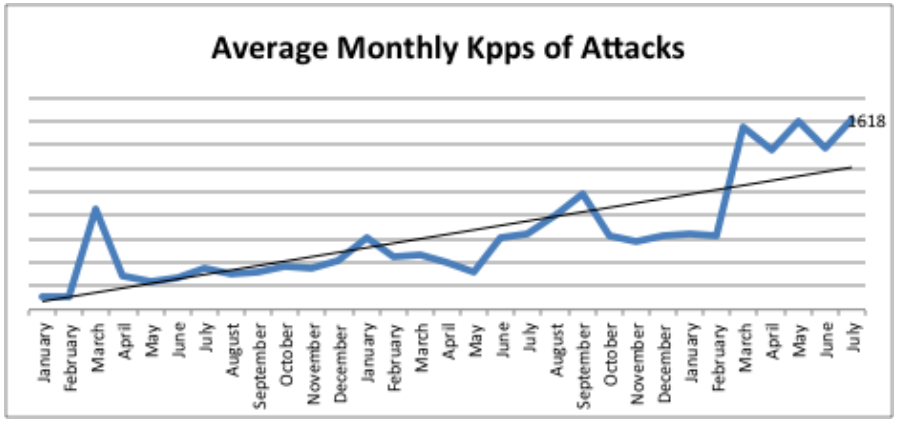


2011 ATLAS Initiative : Anonymous Stats

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





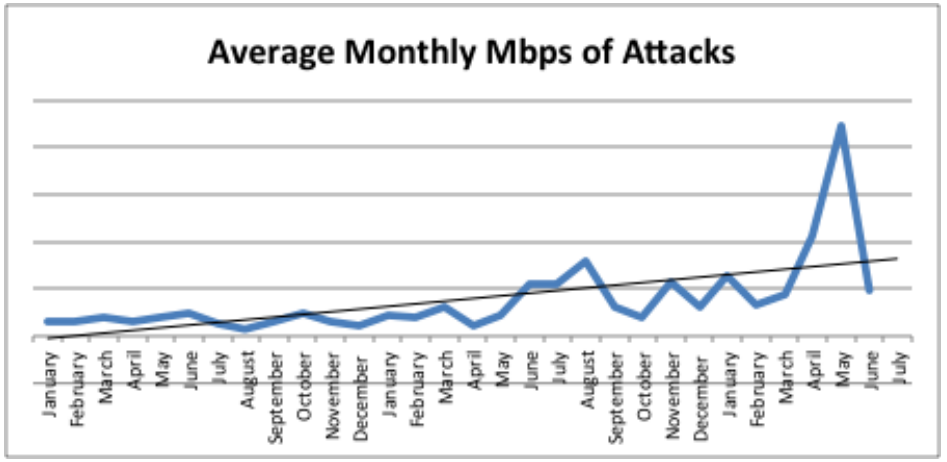
- Average attacks sizes have grown by 40.6% / 165.7% since start of 2010

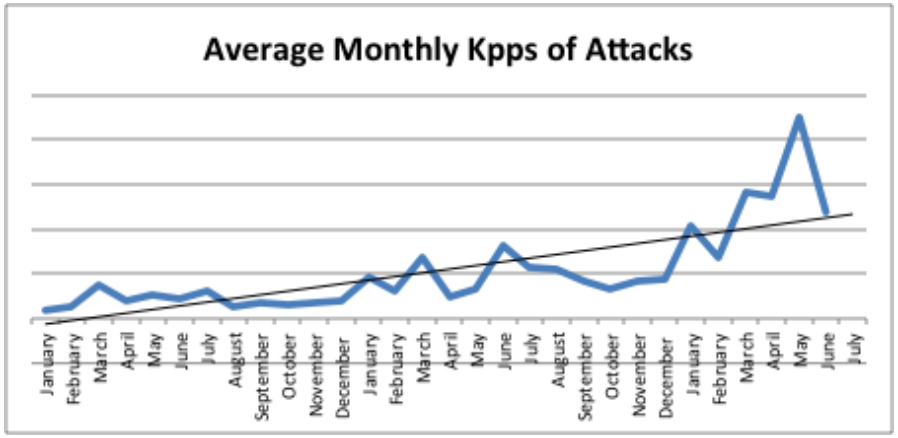
ARBOR NETWORKS

2011 ATLAS Initiative : Anonymous Stats

UK Attack Growth trend in Mbps and Kpps

- Average monthly attack size since start of 2009.
- Average attack is 481.76Mbps / 1.18Mpps, June 2011





- Average attacks sizes have grown by 233% / 1180% since start of 2009
- Spike in May due to a data-collection problem.

ARBOR NETWORKS

2011 ATLAS Initiative : Application Layer Attacks

Continuing to see more application layer attacks

- Arbor customers are detecting / mitigating more application layer attacks:
  - Predominantly targeting HTTP
- Common attack vectors:
  - HTTP GET flood attacks
    - Multiple botnets capable of this.
  - Numerous evolutions of Slowloris / SlowPOST attacks
- Starting to see instances of people using tools with more advanced vectors such as TCP window manipulation / Persist timer attacks, Apache Killer, RefRef etc..
- Increased use of volumetric / state-exhaustion attacks to obfuscate application layer attack vector.

ARBOR NETWORKS

ATLAS Initiative: Key Points

- Majority of attacks are still small (< 1Gbps / < 1Mpps)
  - Proportion of attacks less than 1Gbps / 1Mpss is falling
  - UK following this world-wide trend.
- Proportion of attacks in 2011 over 10Gb/sec seems to be falling, but…
  - Proportion of attacks over 10Mpps is increasing.
  - Have to wait and see for the rest of 2011….
- Largest monitored attack in 2011 (so far) of 65.3Gb/sec & 71.3Mpps
  - Few large attacks monitored for UK.
- 70% of attacks last less than one hour, 77% in UK.
- Average attacks sizes growing world-wide, and for the UK.
- More application layer attacks detected / mitigated.

ARBOR NETWORKS

Questions?
Thank You