ARBOR® NETWORKS

Ninth Annual Worldwide Infrastructure Security Report

Key Findings in the Survey

- DDoS in 2013: Bigger, Broader and Badder
  - Largest attack 3x size of previous years
  - Respondents being targeted at alarming rates
  - Infrastructure again becomes a common target
  - SSL attacks on the rise

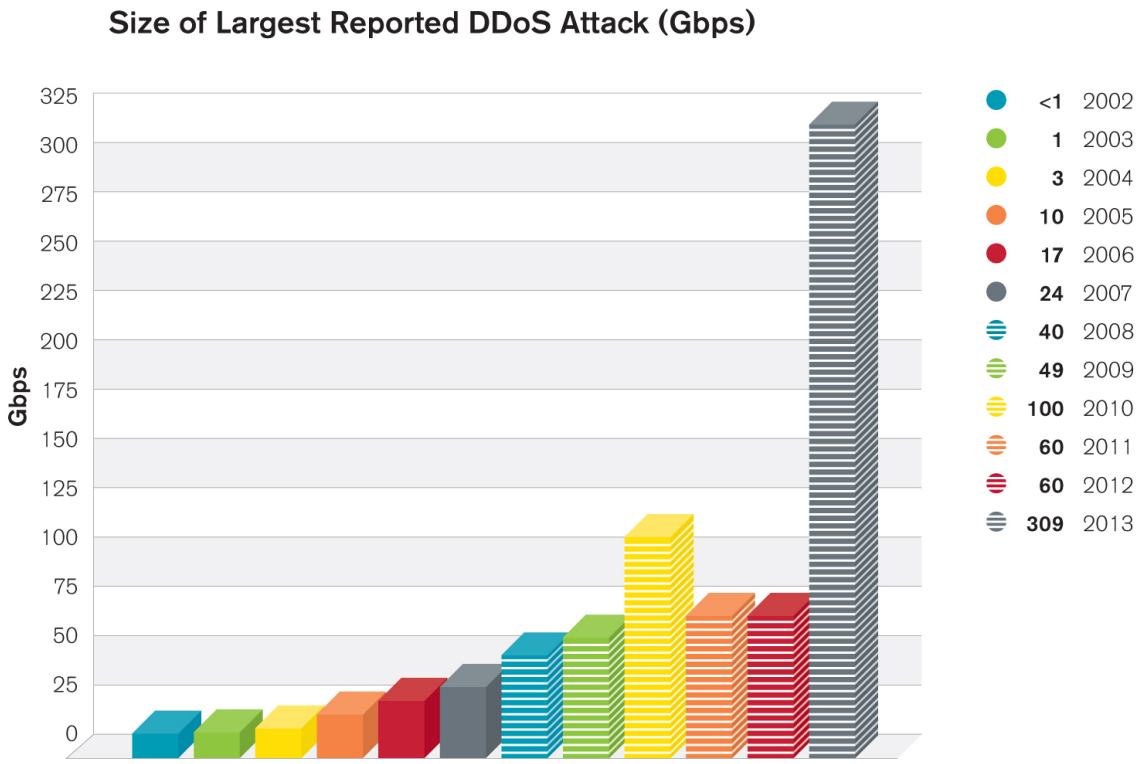
- BYOD Enhances Business while Increasing Risk
  - Nearly three quarters of respondents allow BYOD on internal networks but more than a half have no way of identifying or monitoring them

- Increased Reports of Advanced Persistent Threats (APT)
  - Advanced Persistent Threats (APT) are seen by nearly one third of respondents

Key Findings in the Survey

- Data centers are Continually Victimized
  - Frequency of attacks growing alarmingly with many respondents seeing over 100 attacks per month
  - One third of respondents had attacks that exceeded Internet bandwidth
- Little Improvement Seen in DNS Security Despite Spamhaus and other Large DNS Reflection Attacks
  - Drop in percentage of respondents with dedicated DNS security
- Large Increase in 4G Adoption Significantly Increasing End Point Available Bandwidth
  - Half of the mobile respondents have now rolled out 4G services
- IPv6 Traffic Growing Strongly, but Still not Significant

Substantial Growth in Largest Attacks

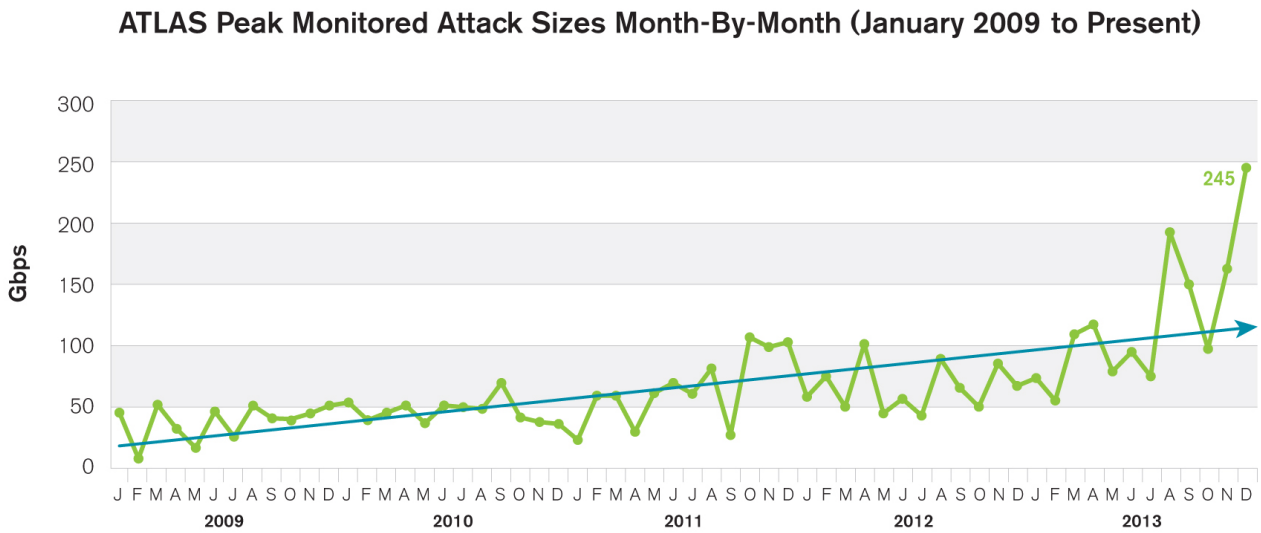


Source: Arbor Networks, Inc.

- Largest reported attacks ranged from 309Gbps at the top end, through 200Gbps, 191Gbps, 152Gbps, 130Gbps and 100Gbps
- Some saw multiple events above 100Gbps but only reported largest

ATLAS Attack Sizes 2013

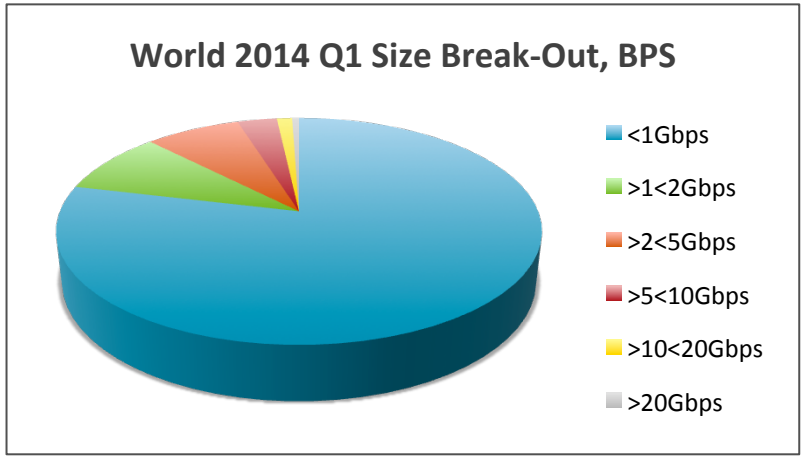
- Peak monitored attack at 245Gbps in 2013, nearly 2.5x last year
  - In-line with growth shown in survey responses
- ATLAS also monitored more than 8x the number of attacks over 20Gbps in 2013, as compared to 2012

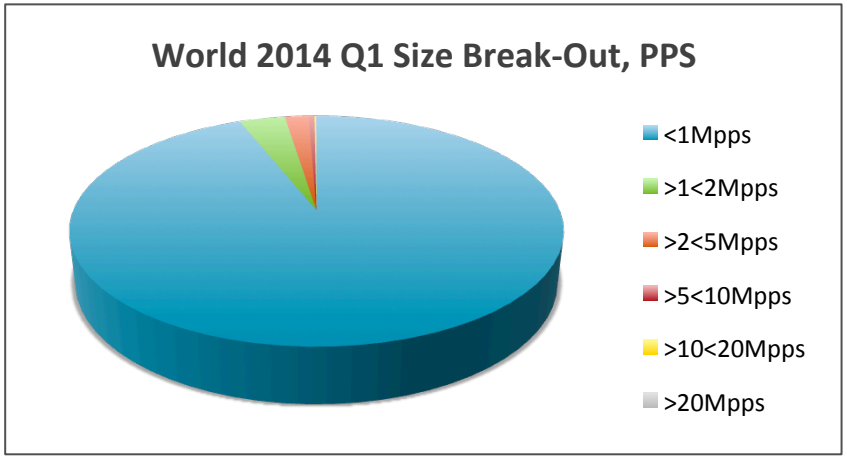


Source: Arbor Networks, Inc.

2014 ATLAS Initiative : Anonymous Stats, World-Wide

- First quarter of new ATLAS data-set
- Focus on providing baseline data for future comparisons
  - Some interesting stats though…..
- 2014 Q1 Summary :
  - 2014 Q1 Average:
    - 1.12 Gb/sec
    - 271.68 Kpps
  - 2014 Q1 Peak:
    - 325.06 Gb/sec
    - 161.58 Mpps



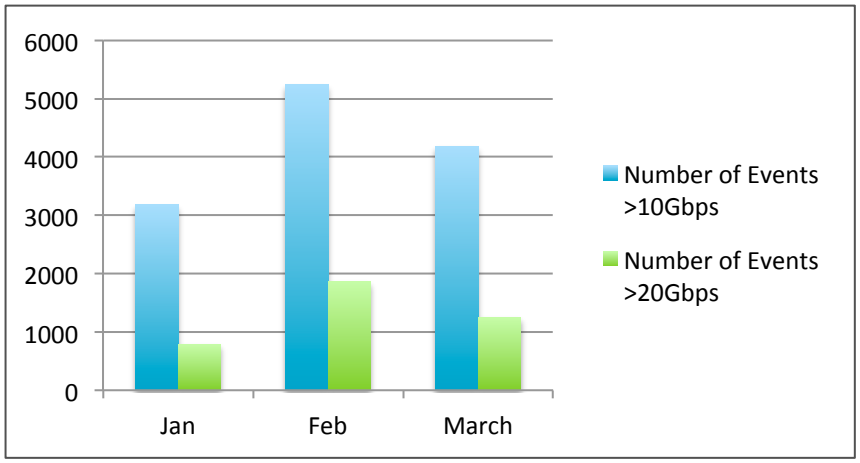


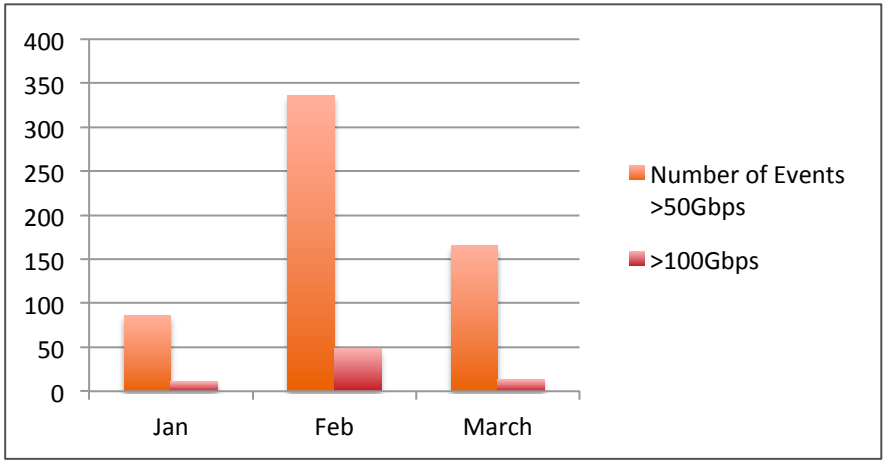
2014 ATLAS Initiative : Anonymous Stats, World-Wide

Large Attacks Multiply

- Already seen nearly 1.5 times the number of events over 20Gbps than seen in whole of 2013!
- And 72 over 100Gb/sec!
- Numbers of events are staggering:
- Predominantly down to proliferation of NTP reflection attacks
  - 14% of events overall
  - 56% of events over 10Gbps
  - 84.7% of events over 100Gbps
- Average event size over 10Gbps = 20.41 Gbps

Q1 Cumulative Large Event Break-Out

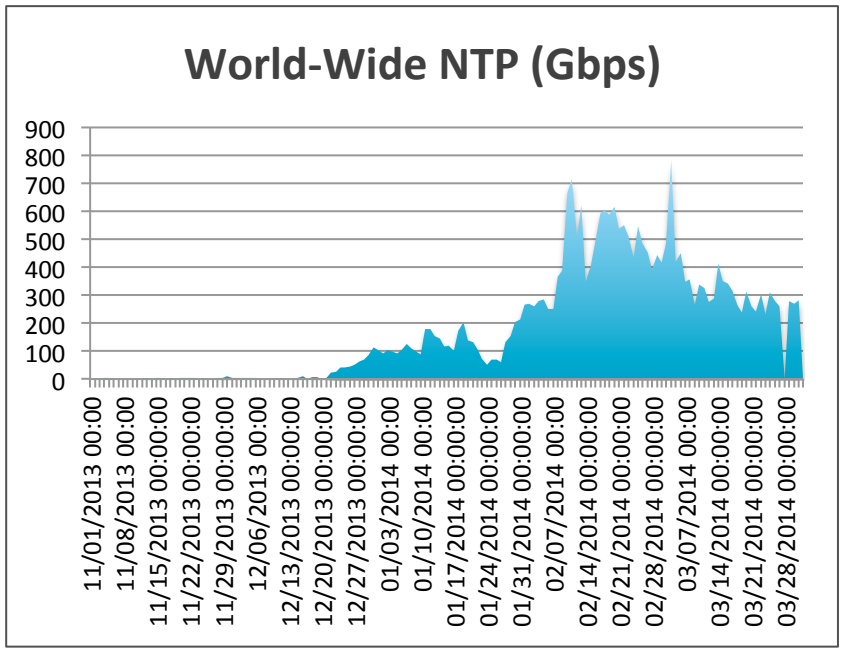


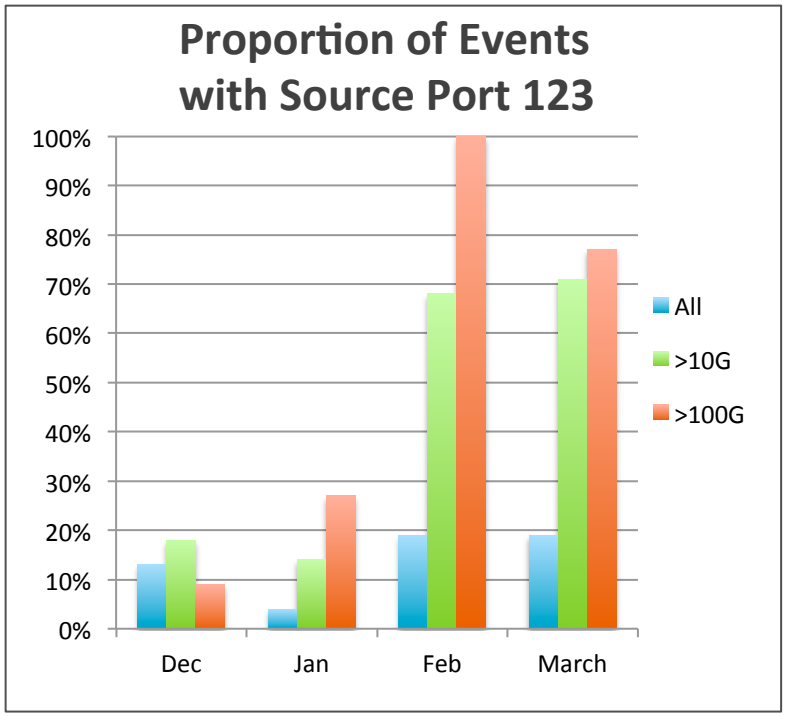


2014 ATLAS Initiative : Anonymous Stats, World-Wide

NTP Reflection / Amplification

- Growth of NTP attacks clearly shown in ATLAS traffic data.
  - Average of 1.29 Gbps NTP traffic globally in November 2013
  - Average of 351.64 Gbps in February 2014
- Cooling off through the end of March
  - Still significantly above 2013 levels





Attack Targets

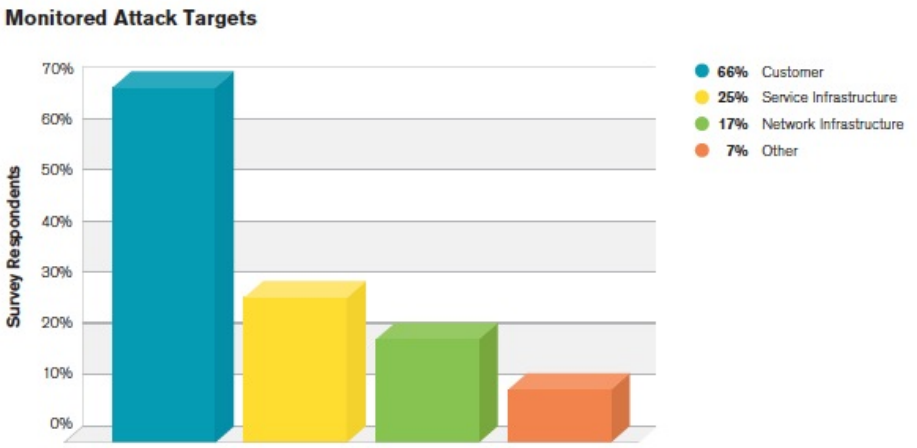


Figure 17 Source: Arbor Networks, Inc.

- Customers of respondents most common targets of attacks
- Significant attacks targeting network infrastructure up from 11% to 17%

- End-Users or subscribers most common target type, financial and e-commerce services tie for second place
- Big increase seen in attacks against financials and government

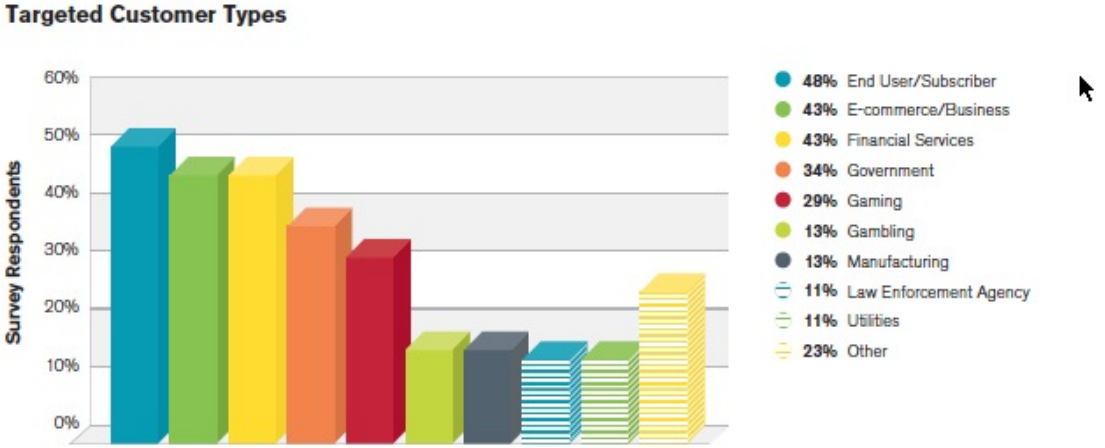
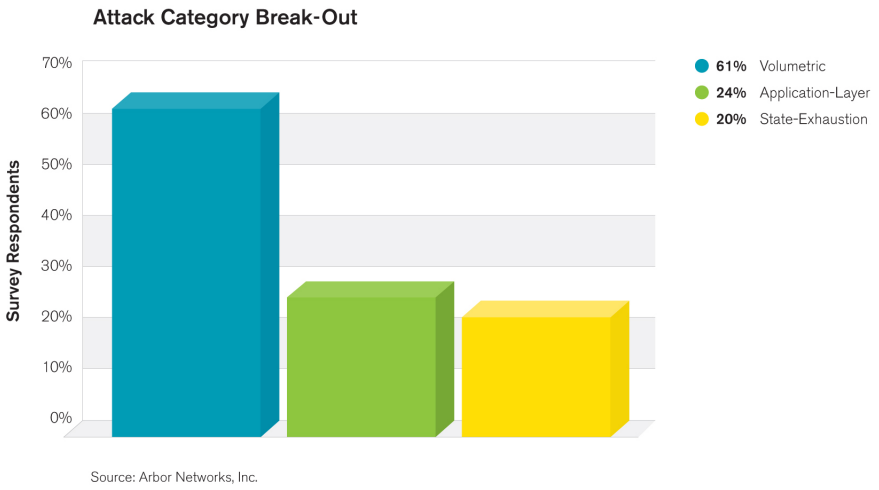
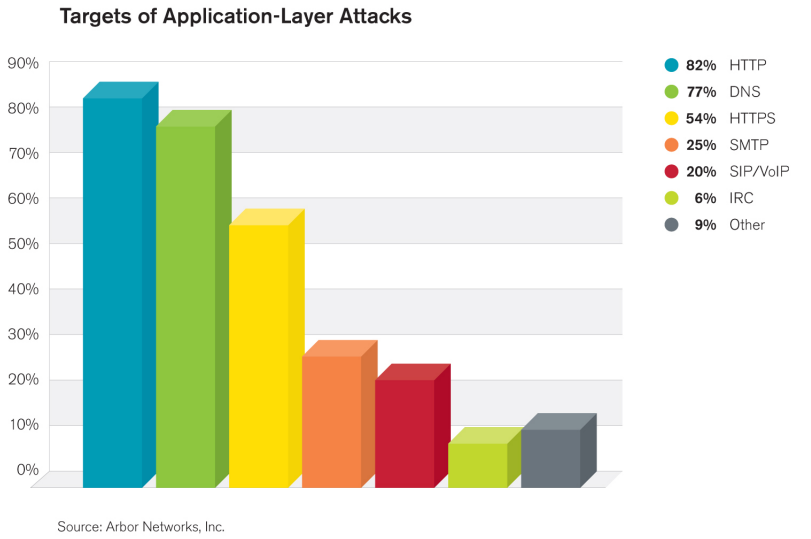


Figure 18 Source: Arbor Networks, Inc.

Application Layer Attacks





- 24% of total attacks seen targeted application-layer
  - 86% of respondents saw some application layer attacks
- 82% reported applications attacks against Web services (HTTP)
  - 77% saw DNS attacks
  - Only 25% reported SMTP attacks
- HTTPS attacks up dramatically at 54% from 37% in 2012 and 24% in 2011

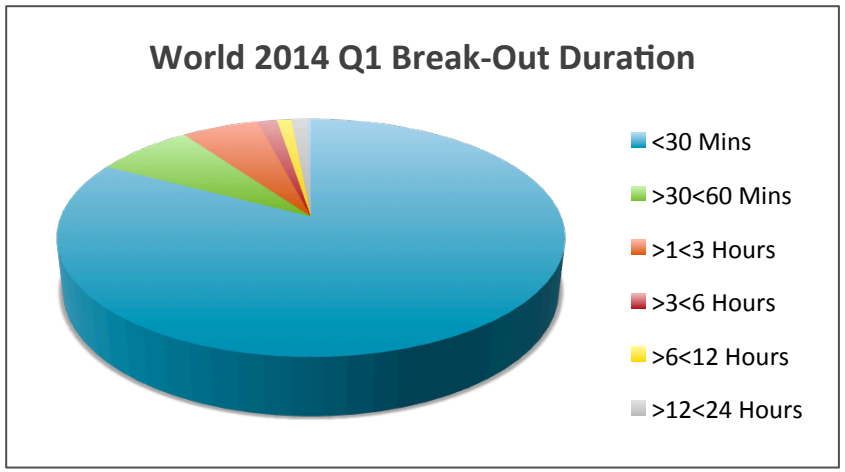
2014 ATLAS Initiative : Anonymous Stats, World-Wide

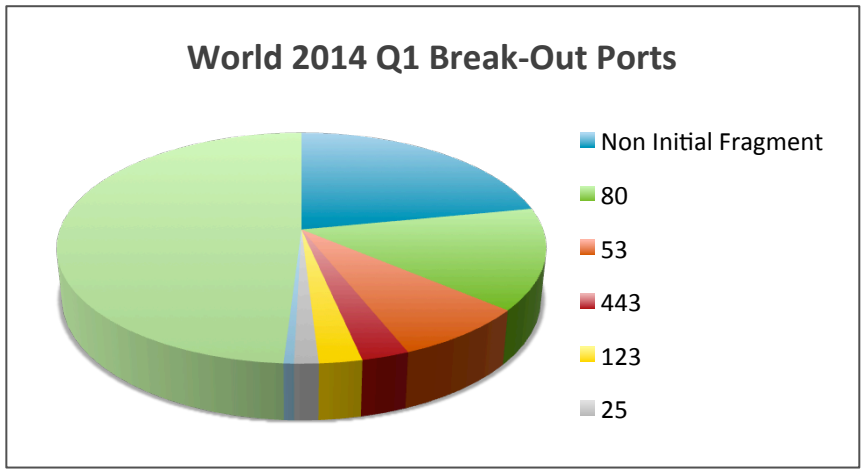
Duration Break-Out

- Majority of attacks short-lived, approx 90.1% less than 1 hour
- Average attack duration 1 hour 0 minutes.
- Average duration of attacks over 10G is 55 minutes.
- Proportion of attacks lasting longer than 12 hours is 1.48%

Dest Port Break-Out

- NIF at number 1, with 22% of events, ports 80 and 53 in second and third place.
- Port 443 (HTTPS) the target in 2.7% of events





Attack Motivations

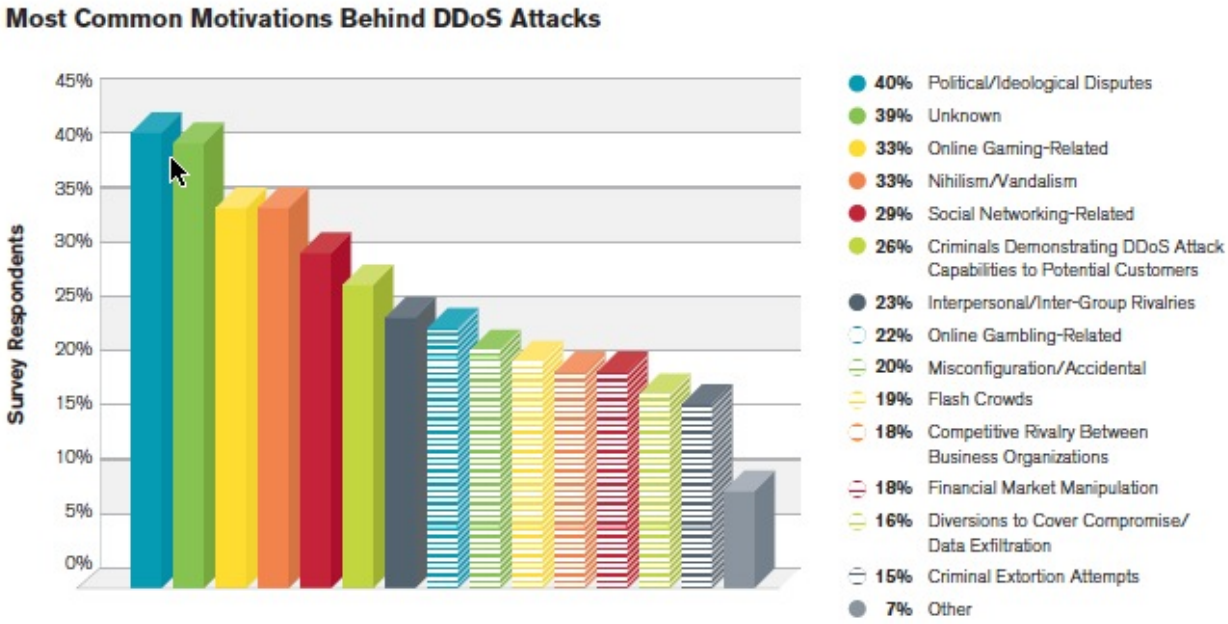
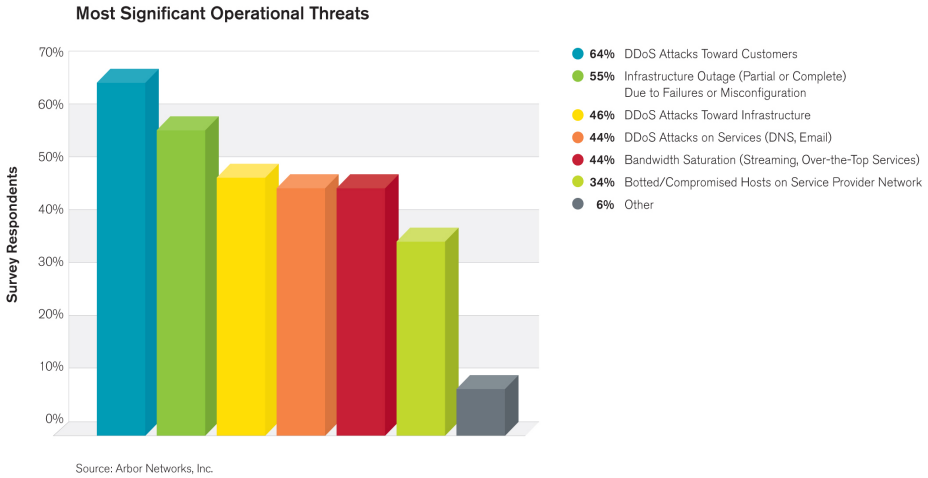
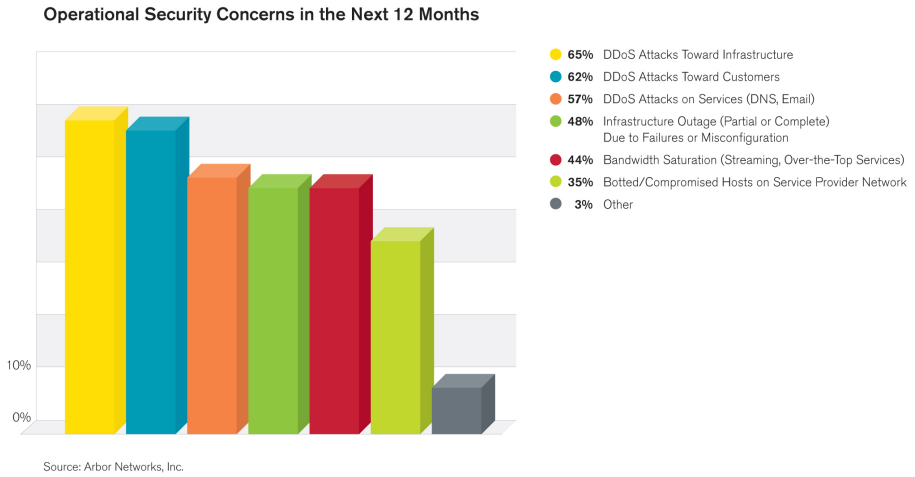


Figure 13 Source: Arbor Networks, Inc.

- Ideological hacktivism continues to be the top perceived motivation, as per the last two years.
- 15-18% of respondents see DDoS being used as a distraction from other criminal activity, such as financial market manipulation or a competitive takeout

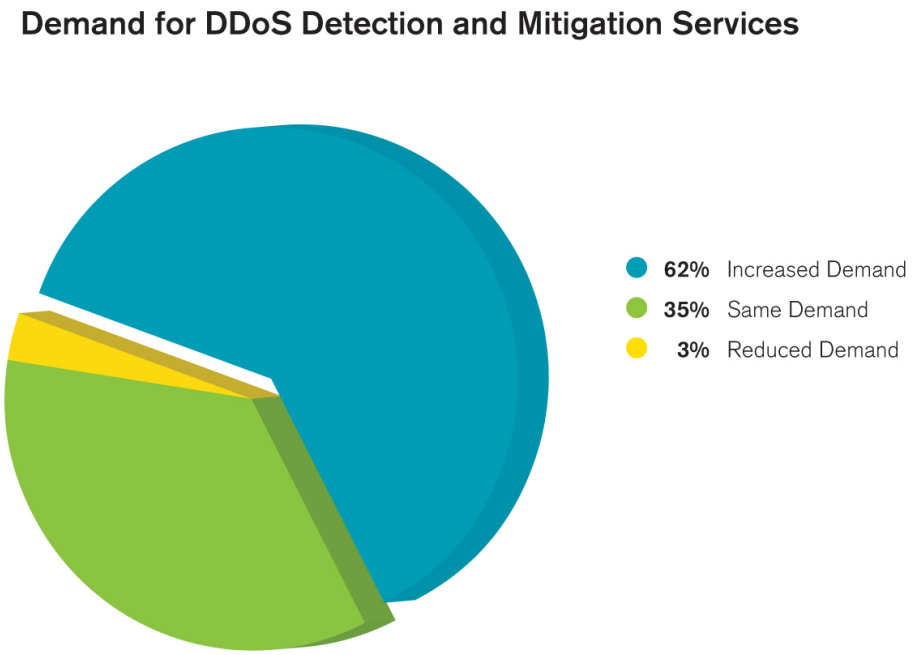
Threats and Concerns





- DDoS attacks against customers are top experienced threat
- Outage due to failure or misconfiguration takes #2 spot at 55%
- Bandwidth congestion due to non-attacks experienced by 44%
- DDoS attacks against infrastructure top concern for this year
- Bandwidth congestion growing concern at 44%, almost 2x last year
- Concerns about failure or misconfiguration still rank 4th, despite ranking 2nd most commonly experienced threat for past 4 years

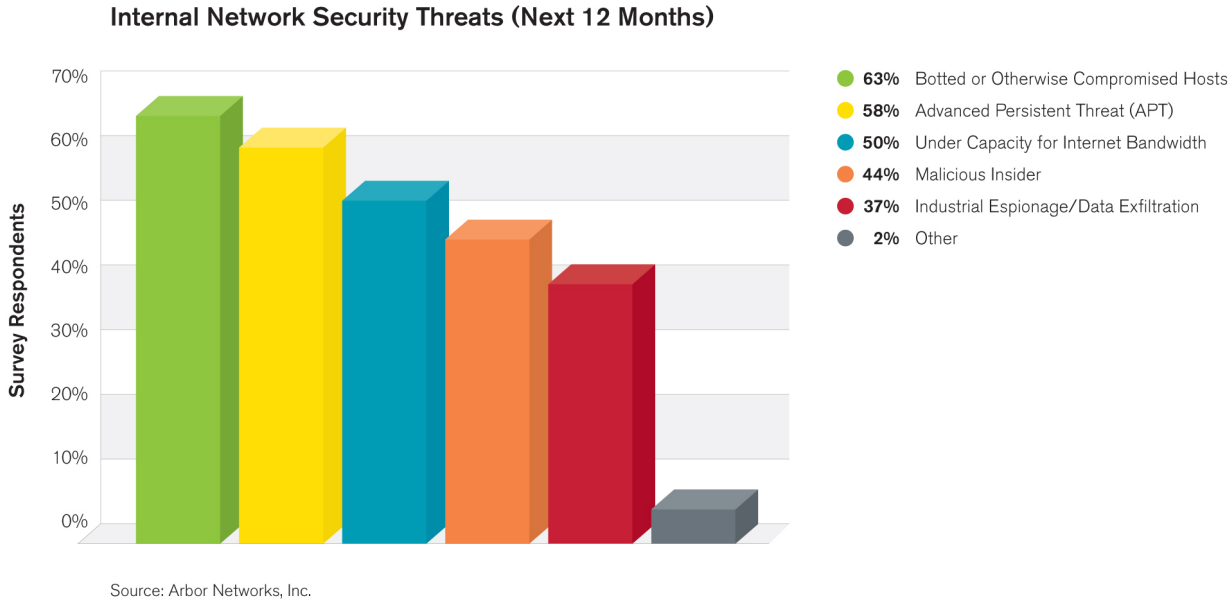
DDoS Top Priority for Customers



Source: Arbor Networks, Inc.

- 62% of service providers see increased demand for DDoS detection and mitigation services from their customers
- 35% see the same demand as in previous years

Corporate Network Threats & Concerns

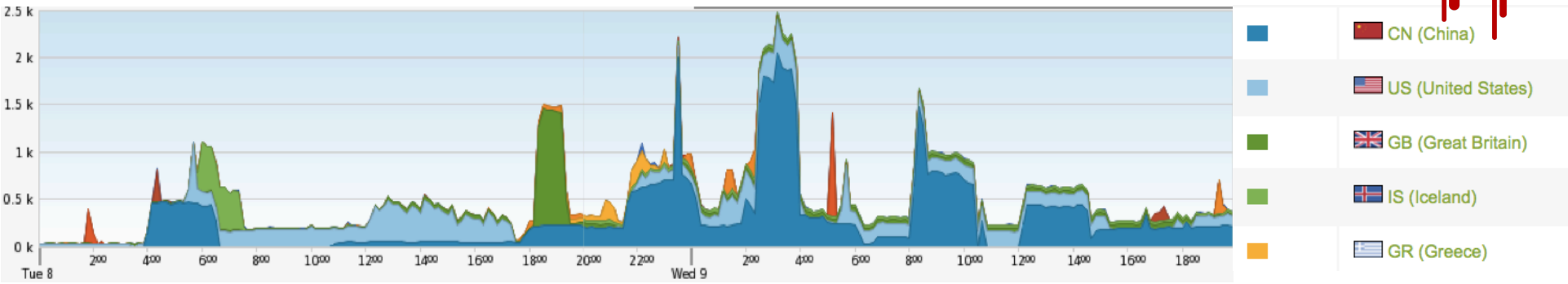


Source: Arbor Networks, Inc.

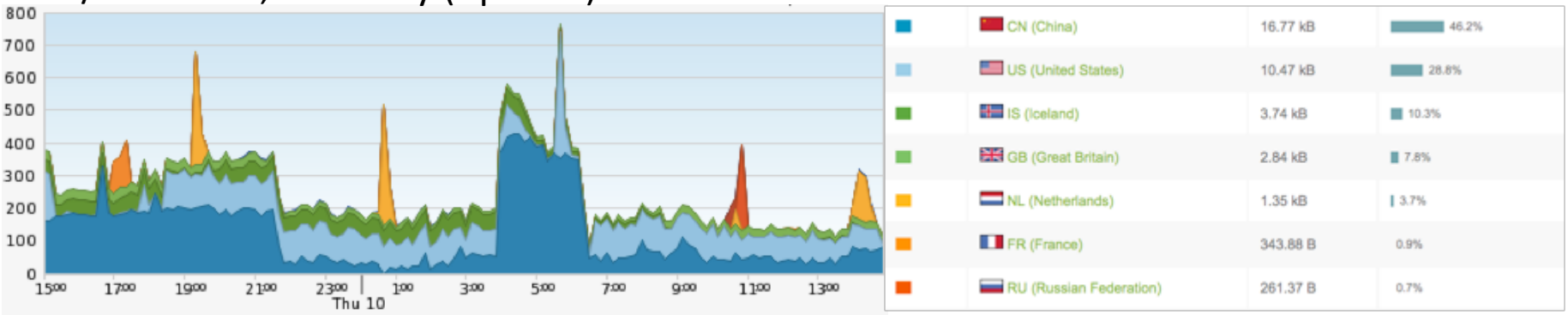
- Top threats for corporate networks were “botted compromised hosts” and “under-capacity for Internet bandwidth”
- 30% report seeing APTs on their networks, up from 20% last year
- Botted hosts once again top concern for 2014
- APTs remain in 2nd place as 2014 concerns

Heartburn Over Heartbleed

TCP/443 scans, Tuesday – Wednesday (April 8-9)

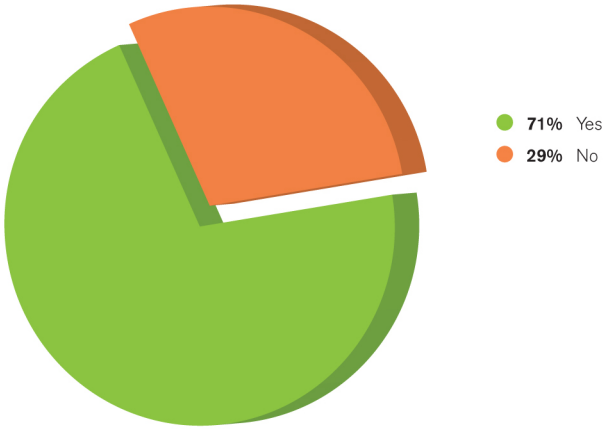


TCP/443 scans, Thursday (April 10)



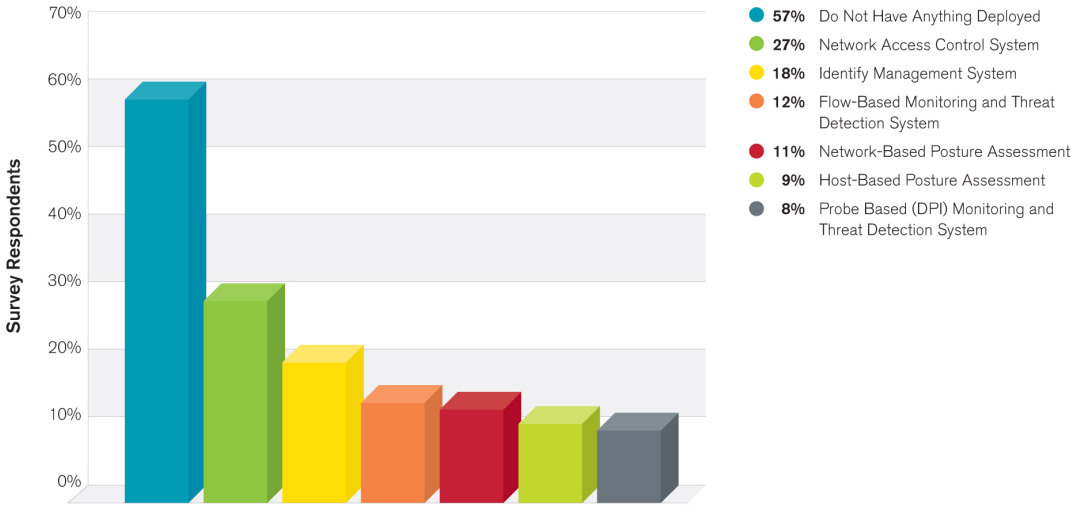
BYOD Proliferation

Use of BYOD



Source: Arbor Networks, Inc.

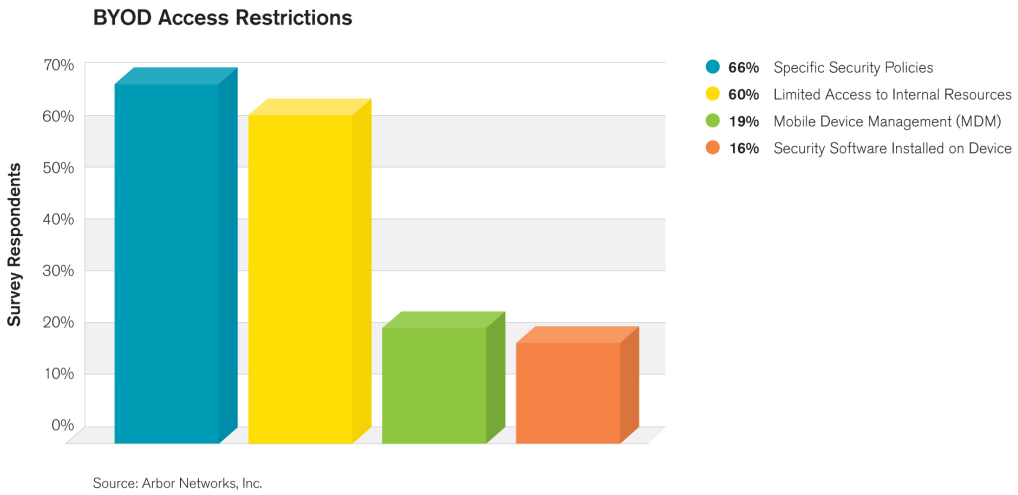
Identification of Employee Owned Device

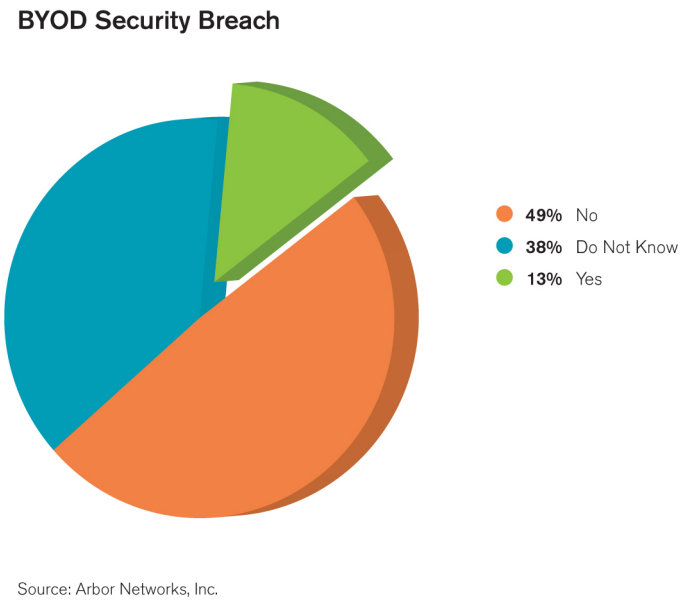


Source: Arbor Networks, Inc.

- Respondents allowing BYOD on internal networks has increased from 63% to 71%
- **57% do not** have a way to identify or monitor these devices
  - Network access control and identity management systems are the two most popular mechanisms.

BYOD Security Risk

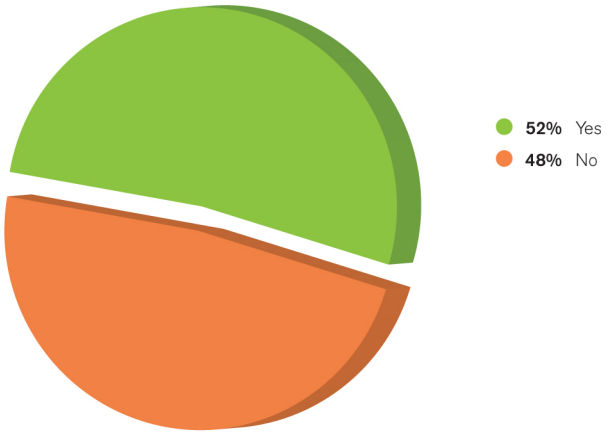




- 13% of respondents experienced a security breach attributed to BYOD
- 39% do not know if they had a security breach due to BYOD practices

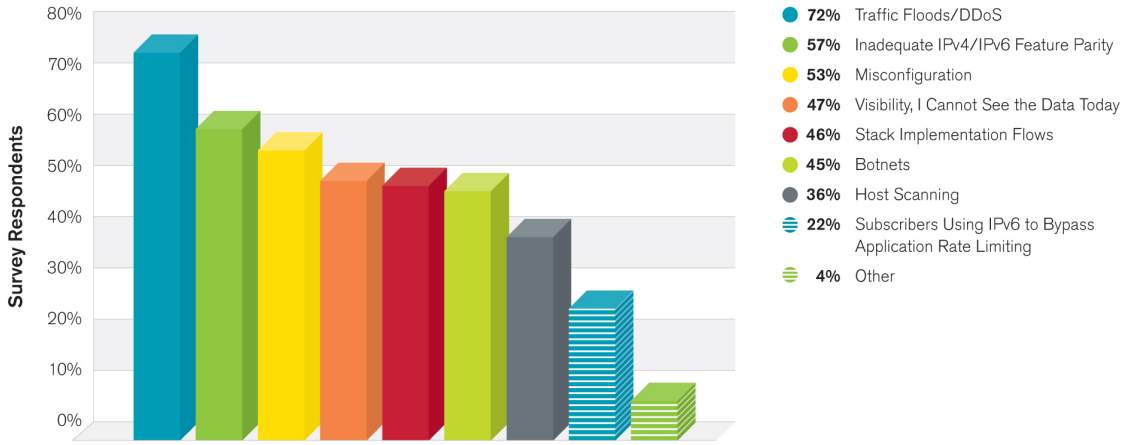
IPv6 Observations

Prevalence of IPv6 Traffic Visibility



Source: Arbor Networks, Inc.

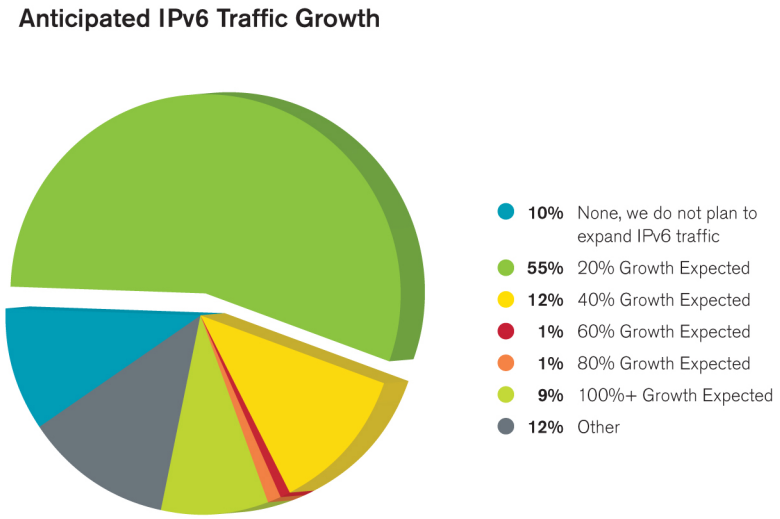
IPv6 Security Concerns



Source: Arbor Networks, Inc.

- Only slightly less than half of respondents have a visibility solution for IPv6
- floods or other DDoS attacks at 72%
- IPv4 and IPv6 feature parity moved up to 2nd place above misconfiguration

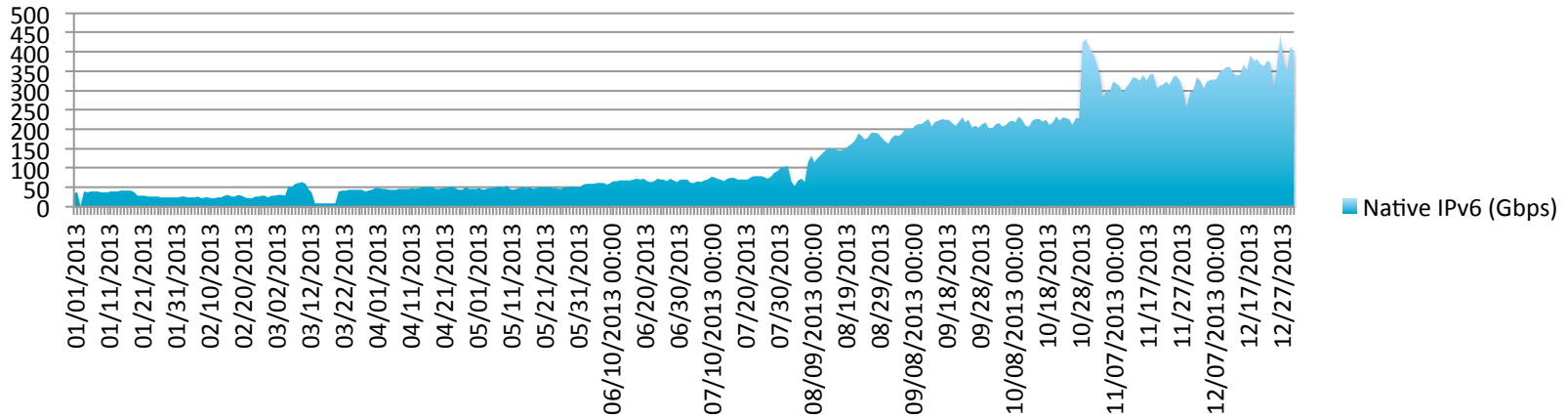
IPv6 Traffic Growth



Source: Arbor Networks, Inc.

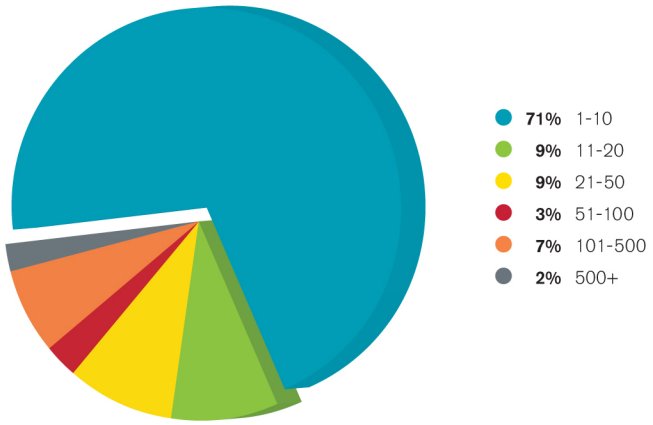
- Largest reported volume of IPv6 traffic monitored was 20Gbps, a massive increase over last year's 3Gbps
- ATLAS shows a **10x** fold increase in monitored native IPv6 traffic growth to a peak of 445Gbps.

Native IPv6 Traffic World-Wide, Gbps



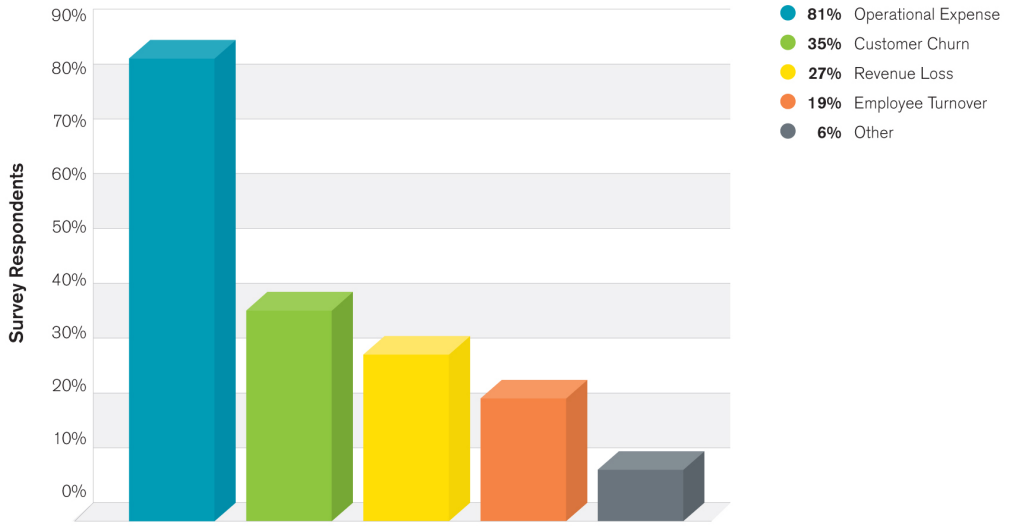
Data Center DDoS Attacks & Impact

Frequency of DDoS Attacks in the Data Center



Source: Arbor Networks, Inc.

Business Impact of DDoS Attacks in the Data Center



Source: Arbor Networks, Inc.

- Nearly ¾ reported DDoS attacks, up from only 45% last year
- 36% see attacks exceed total Internet bandwidth, 2x last year
- Nearly 10 percent see more than 100 attacks per month
- 81% reported operational expenses as a business impact
- 35% reported customer churn and 27% cited revenue loss

Data Center Security & DDoS Mitigation

- 83% have good visibility up to Layer 4 but only 23% have Layer 7 visibility
- Overall increase in all types of security mechanisms deployed
- Firewalls continue to dominate followed by IDS/IPS

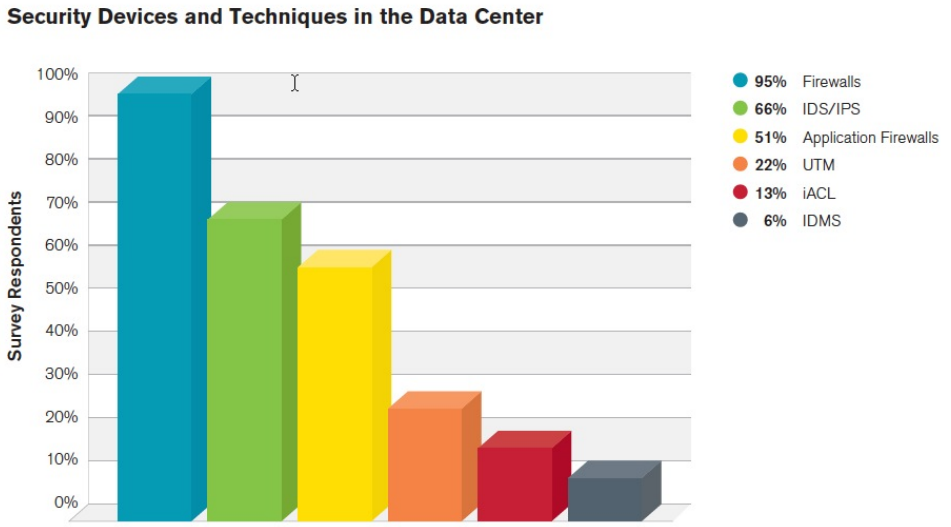
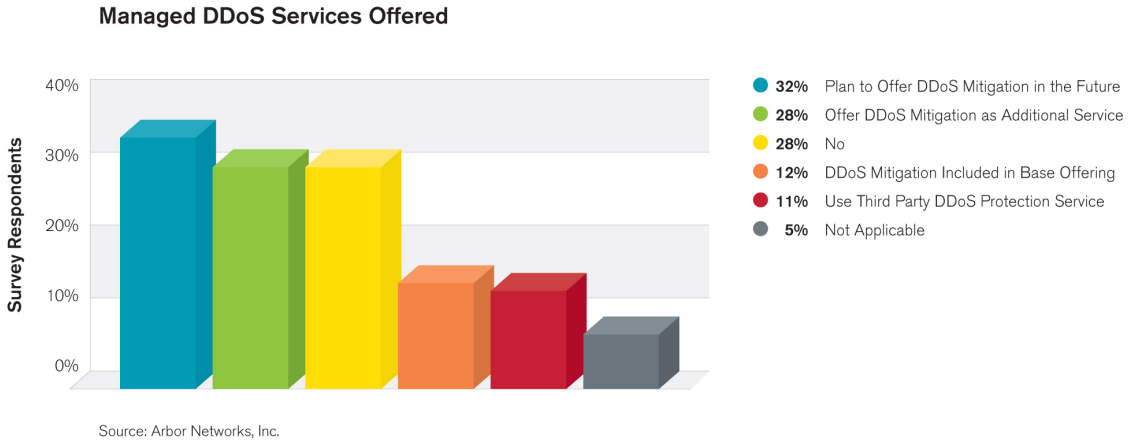


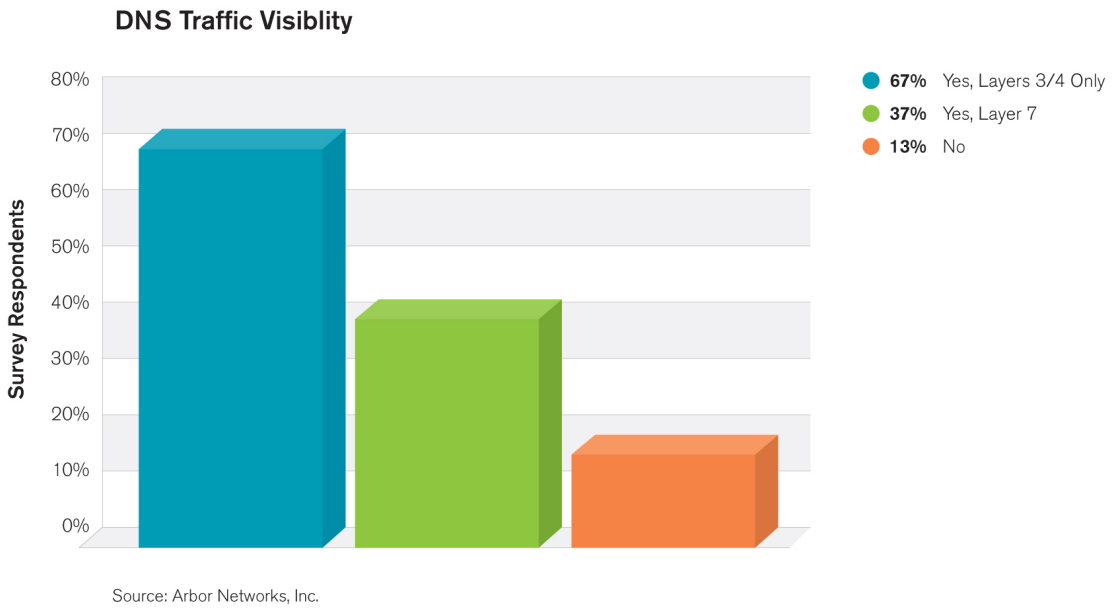
Figure 2 Source: Arbor Networks, Inc.



Source: Arbor Networks, Inc.

- 40% now offer DDoS mitigation & 32% plan future service

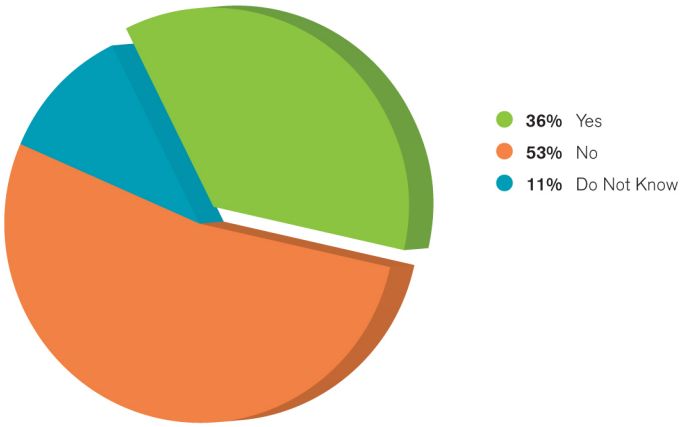
DNS Visibility



- 85% of respondents operate DNS servers on their networks
- 26% have NO security group with formal responsibility for DNS security
- Visibility at Layer 3/4 remains virtually unchanged at 67%
- Layer 7 visibility improved to 37% from 27% last year

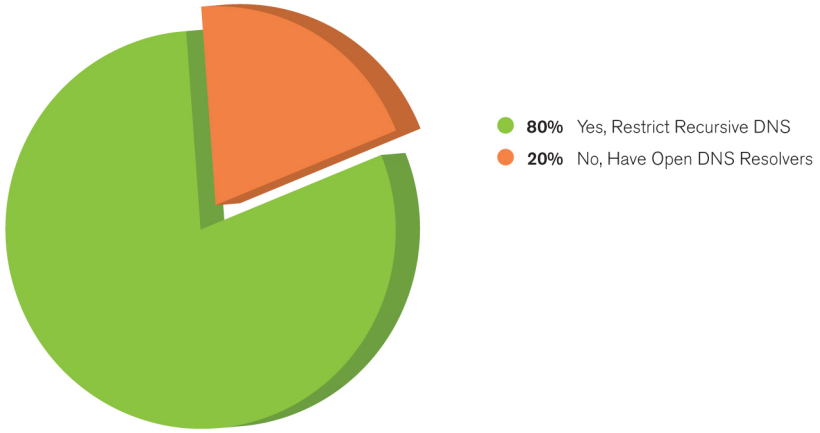
DNS Security

Customer Impacting DNS Attacks



Source: Arbor Networks, Inc.

DNS Recursive Lookups Restricted

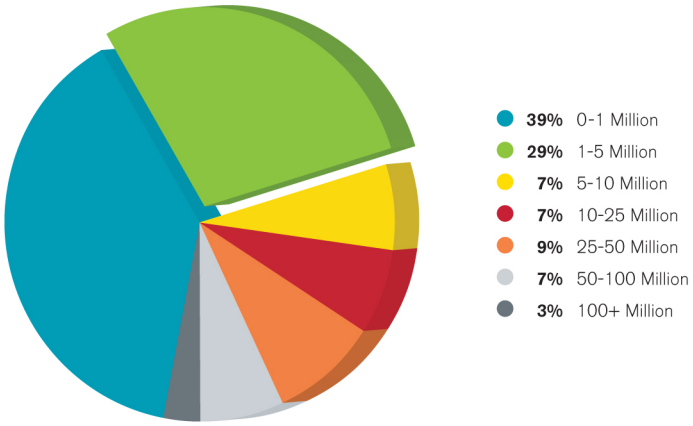


Source: Arbor Networks, Inc.

- 36% of respondents experienced customer-impacting DDoS attacks against DNS infrastructure, an increase of 10 percent over last year
  - 35% saw attacks against authoritative servers
  - 23% saw attacks against recursive servers
- 20% of respondents do NOT restrict recursive look-ups (3 yr. trend)
- 26% have concerns about DNSSEC
  - “New and exciting ways for critical infrastructure service to break.”

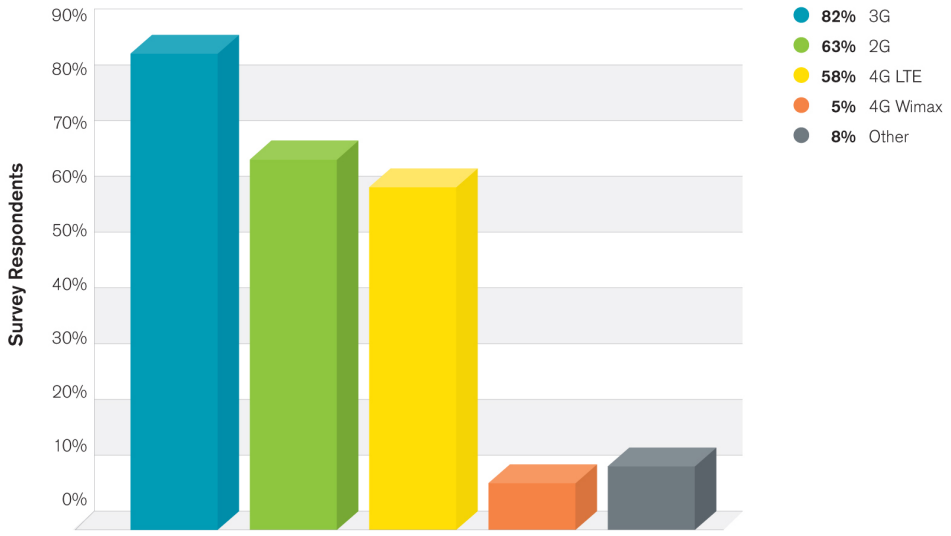
Mobile Respondents and Technologies

Mobile Network Subscribers



Source: Arbor Networks, Inc.

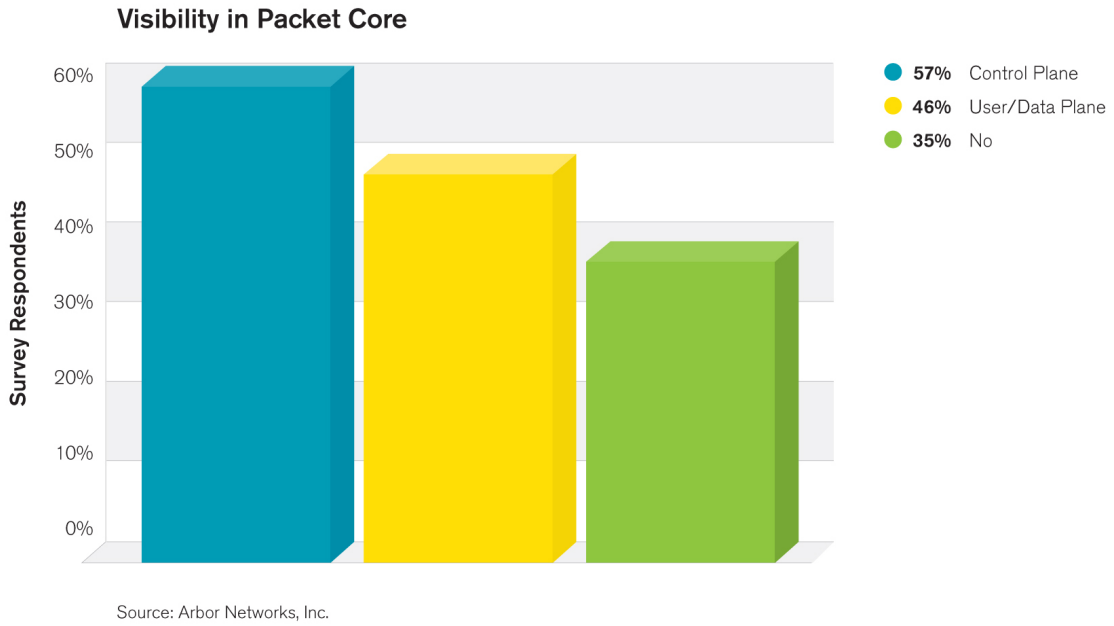
Mobile Technologies Deployed



Source: Arbor Networks, Inc.

- 42% of respondents operate mobile networks, up from 32% last year
  - 60% of these have over 1 Million Subscribers
- LTE deployments continue rapid growth trend
- Nearly half already offer LTE services, with a further 14% planning services for this year

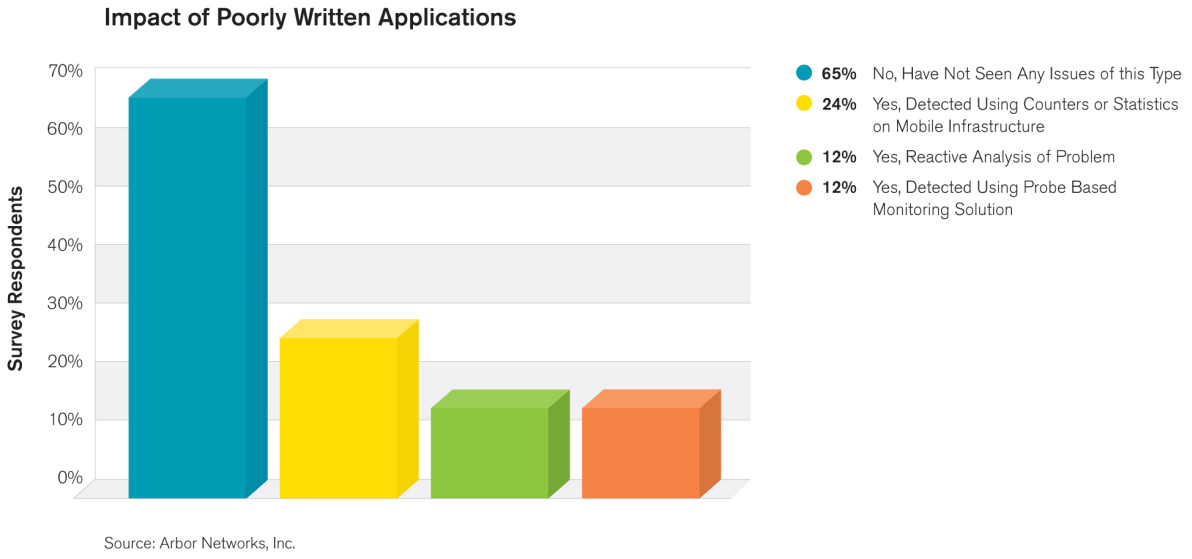
Mobile Packet Core Visibility Improvements



- A huge improvement in visibility. 65% have visibility into their mobile/evolved packet core, up from 40% last year
- 46% now have visibility into the user/data-plane, up from 33% last year
- 57% now have visibility into the control-plane traffic, up from 27% last year

Mobile Network Security

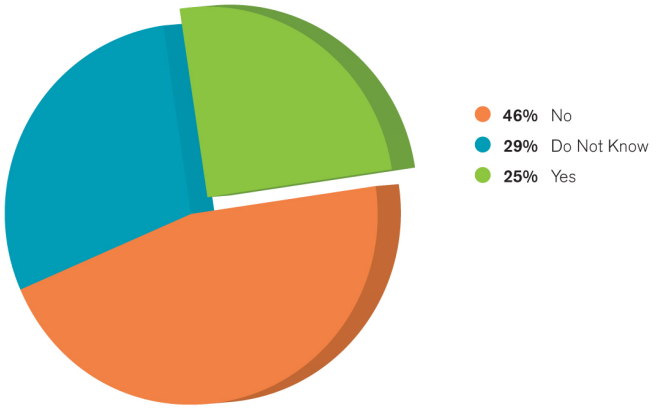
- Over 20% of respondents indicated that they have suffered a customer-visible outage due to a security incident
- Over 63 percent of respondents do NOT know what proportion of subscriber devices on their networks are compromised and are participating in botnets or other malicious activities.
  - An increase from 57 percent



- 35% have experienced poorly implemented mobile applications impacting service

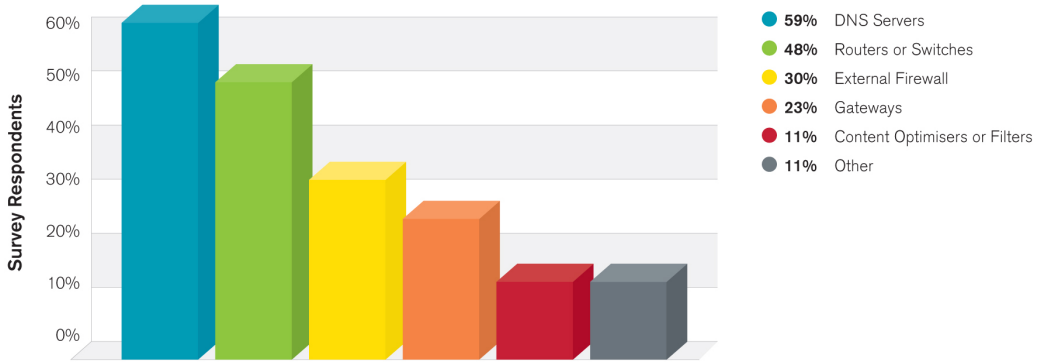
Mobile Threat Detection Improvements

DDoS Attacks on Mobile Networks



Source: Arbor Networks, Inc.

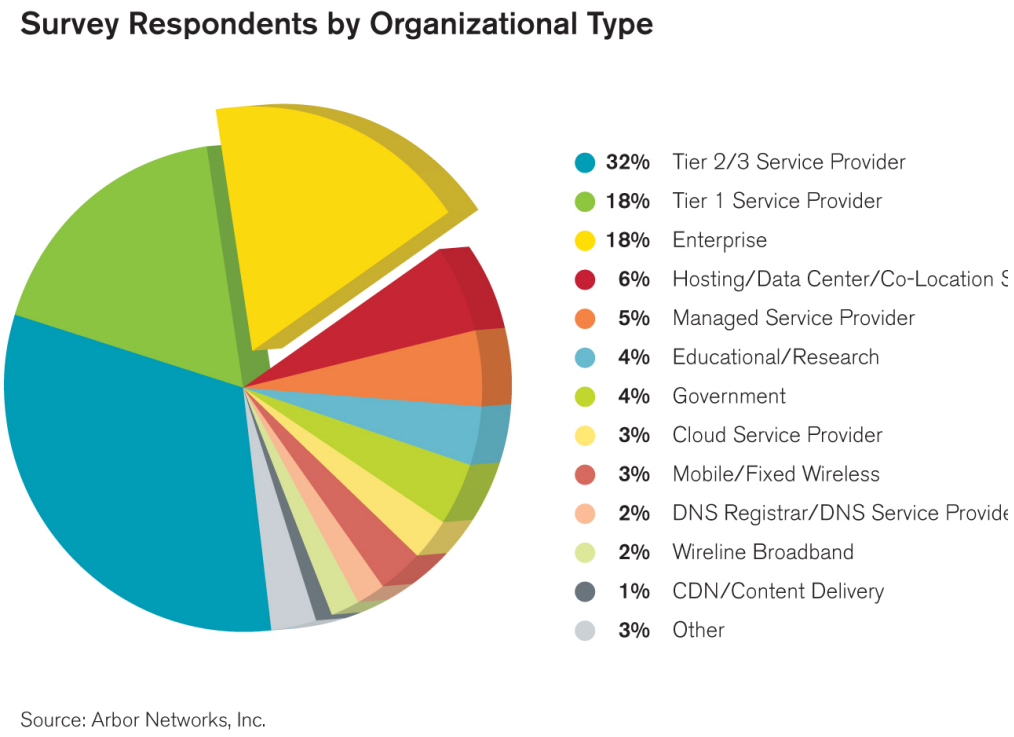
Internet (Gi) Resources Affected by DDoS Attacks



Source: Arbor Networks, Inc.

- 25% of respondents see attacks against their mobile users, RAN, back-haul or packet core but 29% still don't know due to lack of visibility
- 24% see attacks on the Internet (Gi) Infrastructure, up sharply from last year's 10%
- DNS servers most common target

Infrastructure Survey Demographics

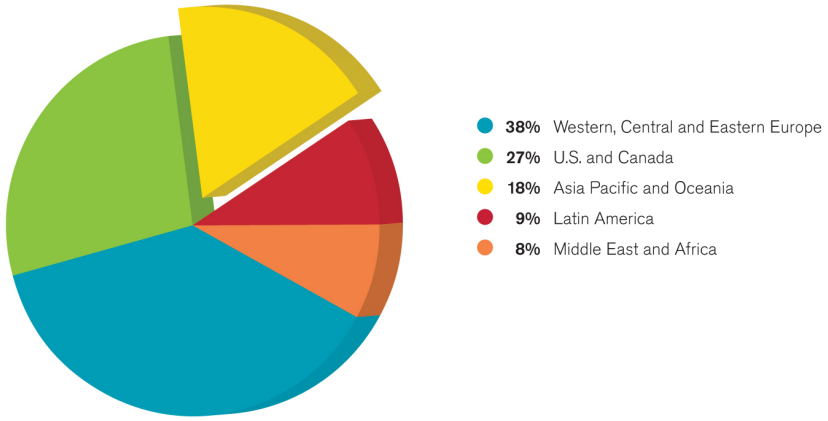


Source: Arbor Networks, Inc.

- Survey conducted in October 2013
- 220 total respondents across different market segments
- More than 70% Internet Service Providers

Infrastructure Survey Demographics

Geographic Distribution of Organizational Headquarters

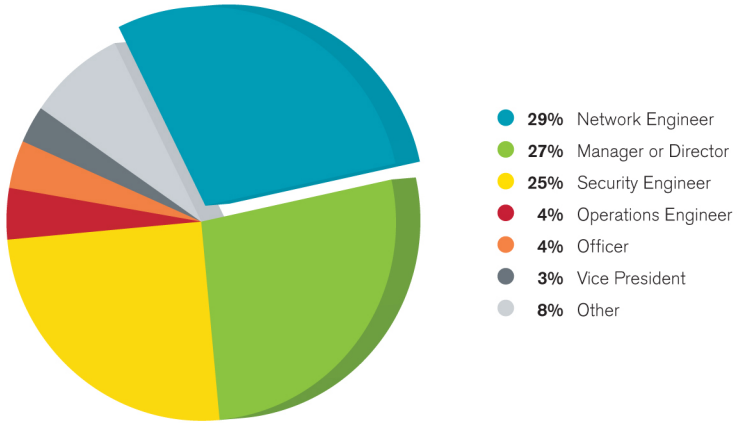


Source: Arbor Networks, Inc.

Geographic distribution

- 38% Europe
- 27% US and Canada
- 18% Asia Pacific
- 9% Latin America
- 8% Middle East / Africa

Role of Respondent

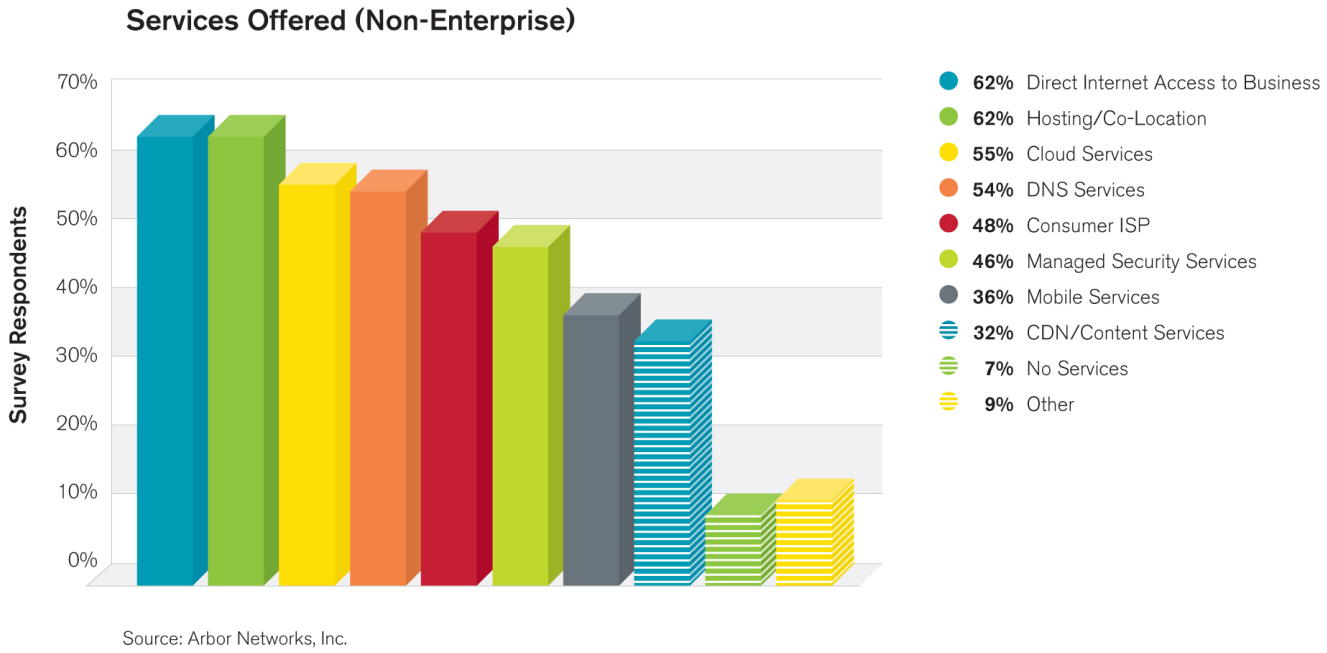


Source: Arbor Networks, Inc.

Role of respondent

- 58% of respondents are network, security or operations engineers
- 34% of respondents are management or executives

Infrastructure Survey Demographics

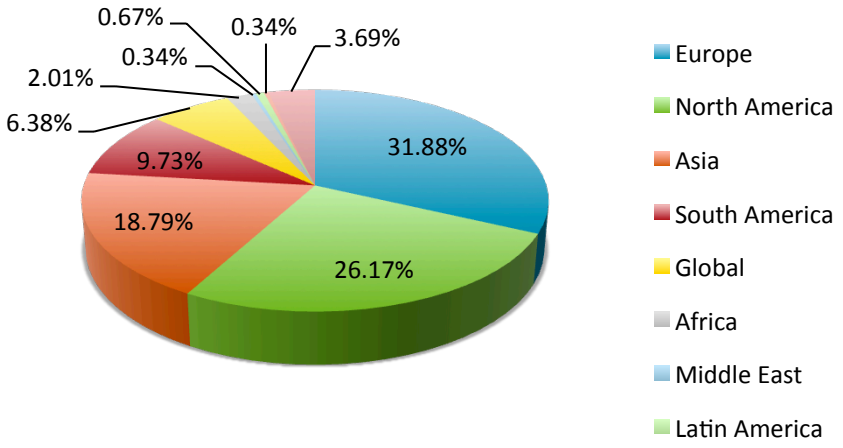


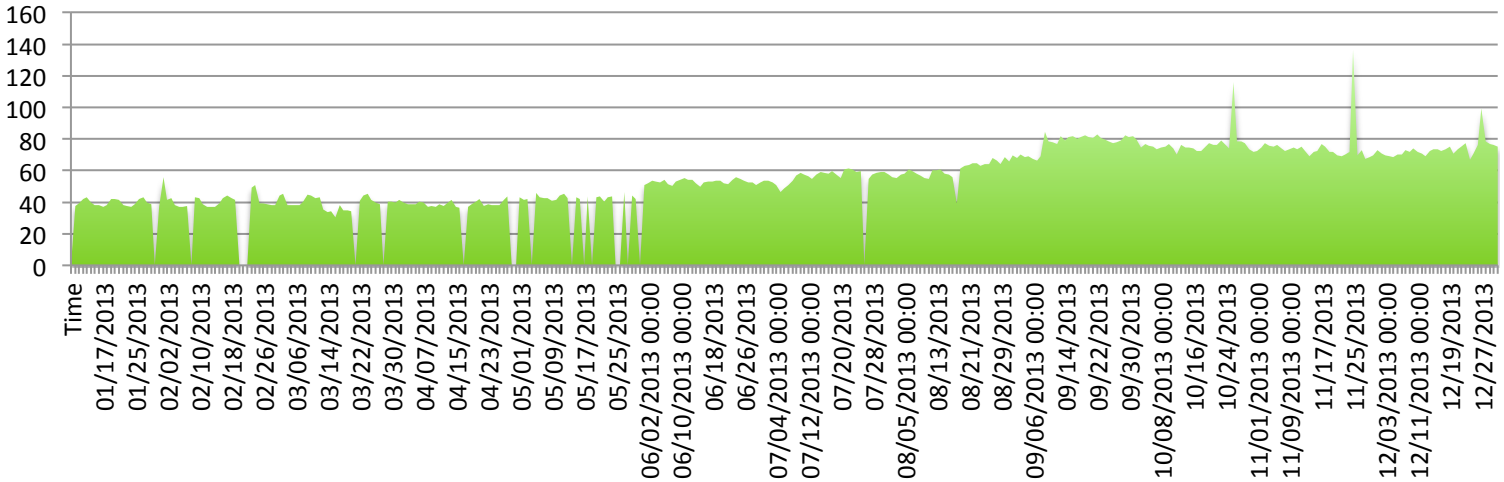
Source: Arbor Networks, Inc.

- Multiple services offered by most respondents
- Internet access and hosting co-location services most common
- Over half offer cloud and DNS services

ATLAS Demographics

- ATLAS provides invaluable data to Arbor customers and the broader operational security community
- 290+ participating networks
  - 32% Europe
  - 26% North America
  - 19% Asia
  - 19% South America
- Tracking a peak of over 80Tbps





ARBOR®
NETWORKS

Thank You