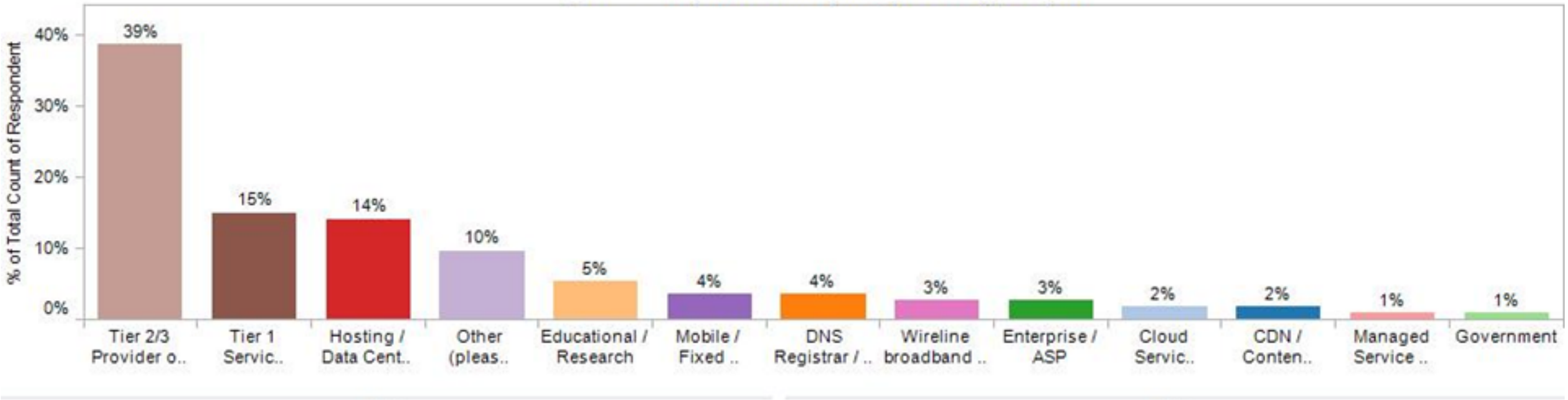
ARBOR NETWORKS

2011 Infrastructure Security Report

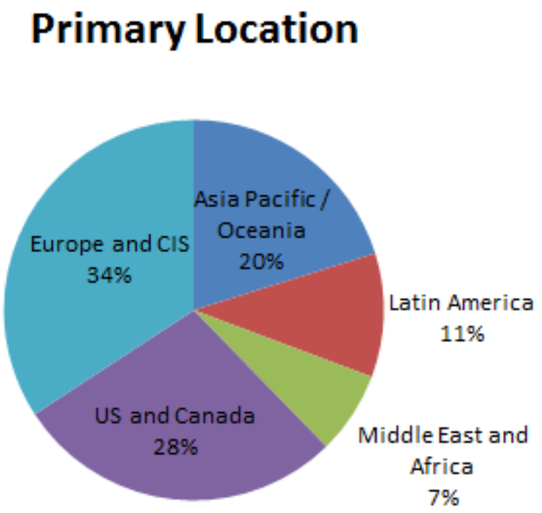
7th Annual Edition

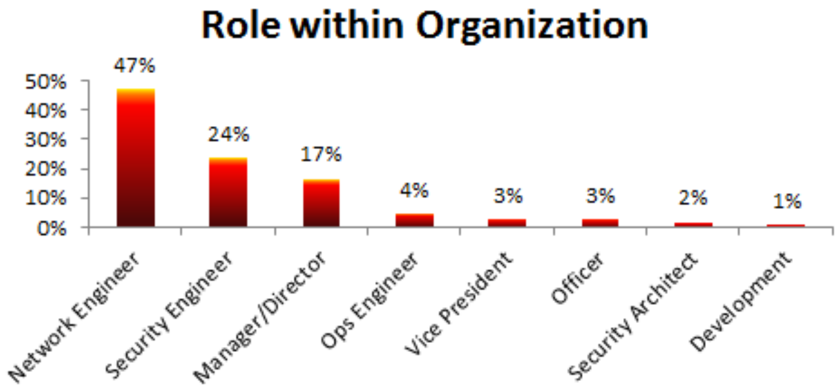
2011 Infrastructure Security Survey



- Survey conducted in October through November 2011
- 114 total respondents across different market segments
- 54% service providers, 15% T1 providers
- “Other” includes VOIP, wholesale internet, DDoS mitigation, database repository payment and credit sites

Survey Demographics





- **Geographic distribution**
  - 41% EMEA
  - 28% US and Canada
  - 11% Latin America
  - 20% APAC
- **77% of respondents network, security, operations engineers, analysts or architects**
- **23% of respondents management or executives**

Key Findings in the Survey

- **Any Internet Operator Can Be a Target for DDoS**
  - *Ideologically-motivated ‘Hacktivism’ and On-line vandalism DDoS attacks are the most commonly identified attack motivations*

- **Size and Scope of Attacks Continue to Grow at an Alarming Pace**
  - *High-bandwidth DDoS attacks are the ‘new normal’ as over 40% of respondents report attacks greater than 1 Gbps and 13% report attacks greater than 10Gbps*
  - *Increased sophistication and complexity of layer-7 DDoS attacks, multi-vector DDoS attacks becoming more common*

- **First-Ever Reports of IPv6 DDoS Attacks 'in the Wild' on Production Networks**

Key Findings

- **Attackers Are Going Where the Money Is**
  - *Rarity of IPv6-enabled attacks indicative of low IPv6 market penetration and lack of critical mass*

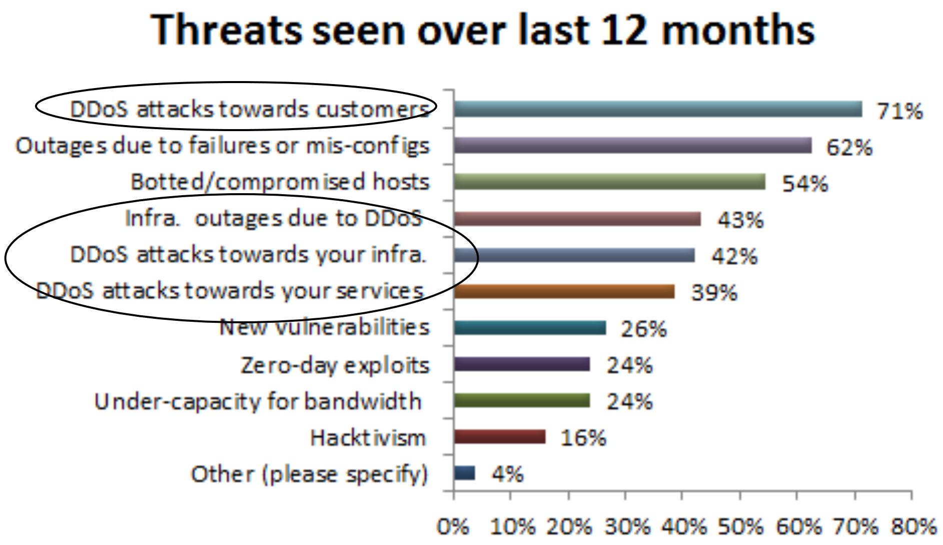
- **Continued Uncertainty Around Visibility & Security of Mobile/Fixed Wireless Networks**

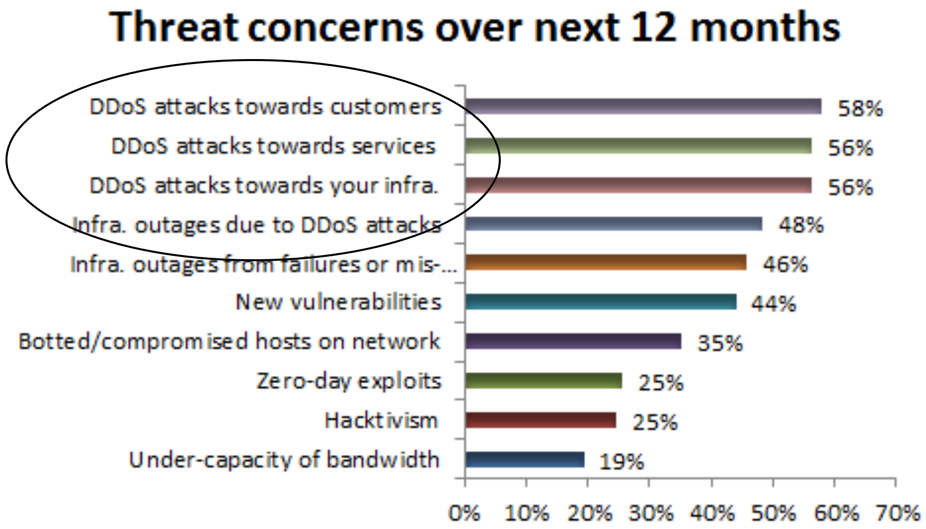
- **Mobile Handsets and Devices Directly Impacted by DDoS Attacks**

- **Trust Issues Abound Across International Boundaries**

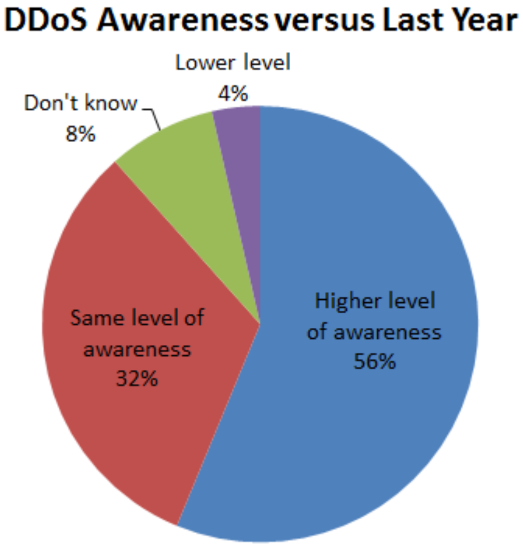
Threats and Concerns

DDoS Threats are Top of Mind


Threats seen over last 12 months

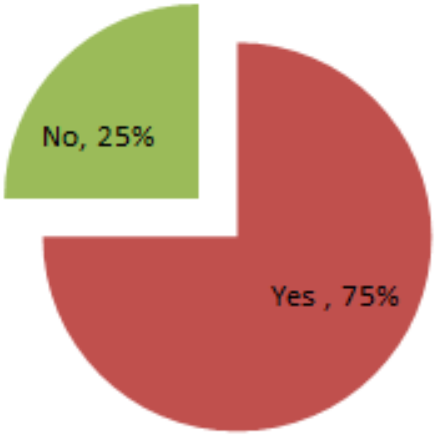

Threat concerns over next 12 months

- 4 of the top 6 threats seen over the last 12 months are DDoS related
- The top 4 perceived threats for the next 12 months are DDoS related
- DDoS threat awareness is high

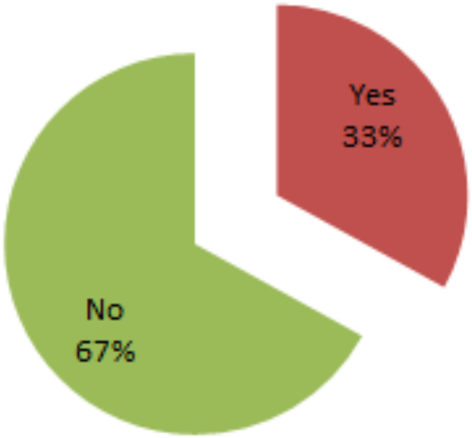

DDoS Awareness versus Last Year

Trust Issues across International Boundaries

Is Traffic Sourced from some Geographical Origins Considered more of a threat?



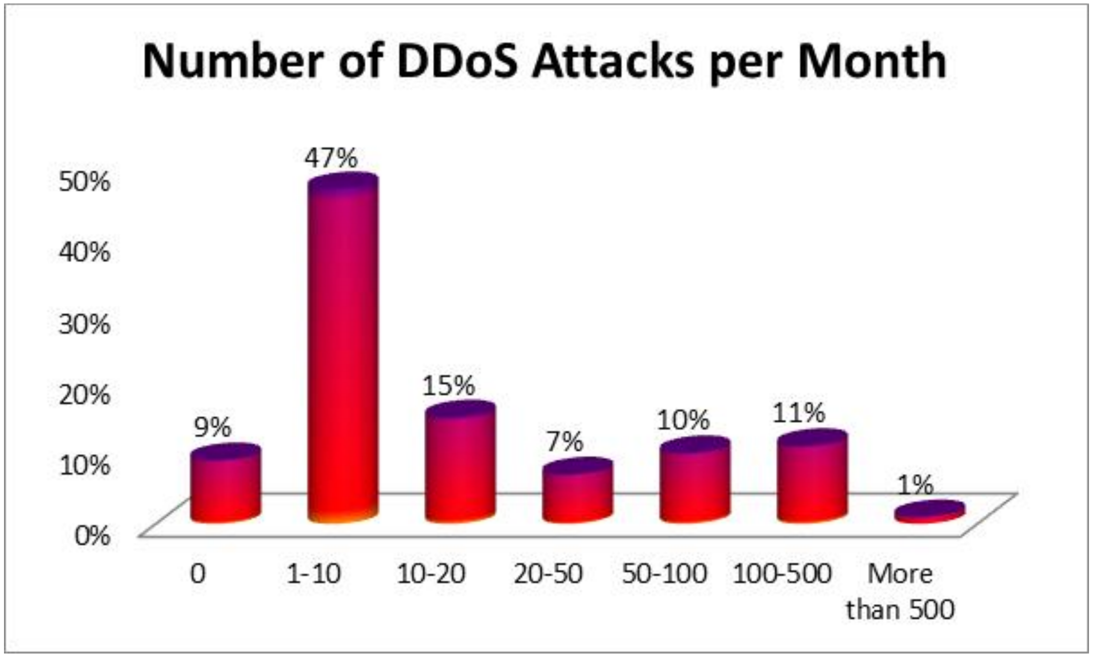
Concerns over National Origins of Equipment being Deployed



- National origins of equipment and geographical traffic sources are still being scrutinized closely
- 75% of respondents consider traffic from some geographical origins a bigger threat and 33% have concerns over vendor origins

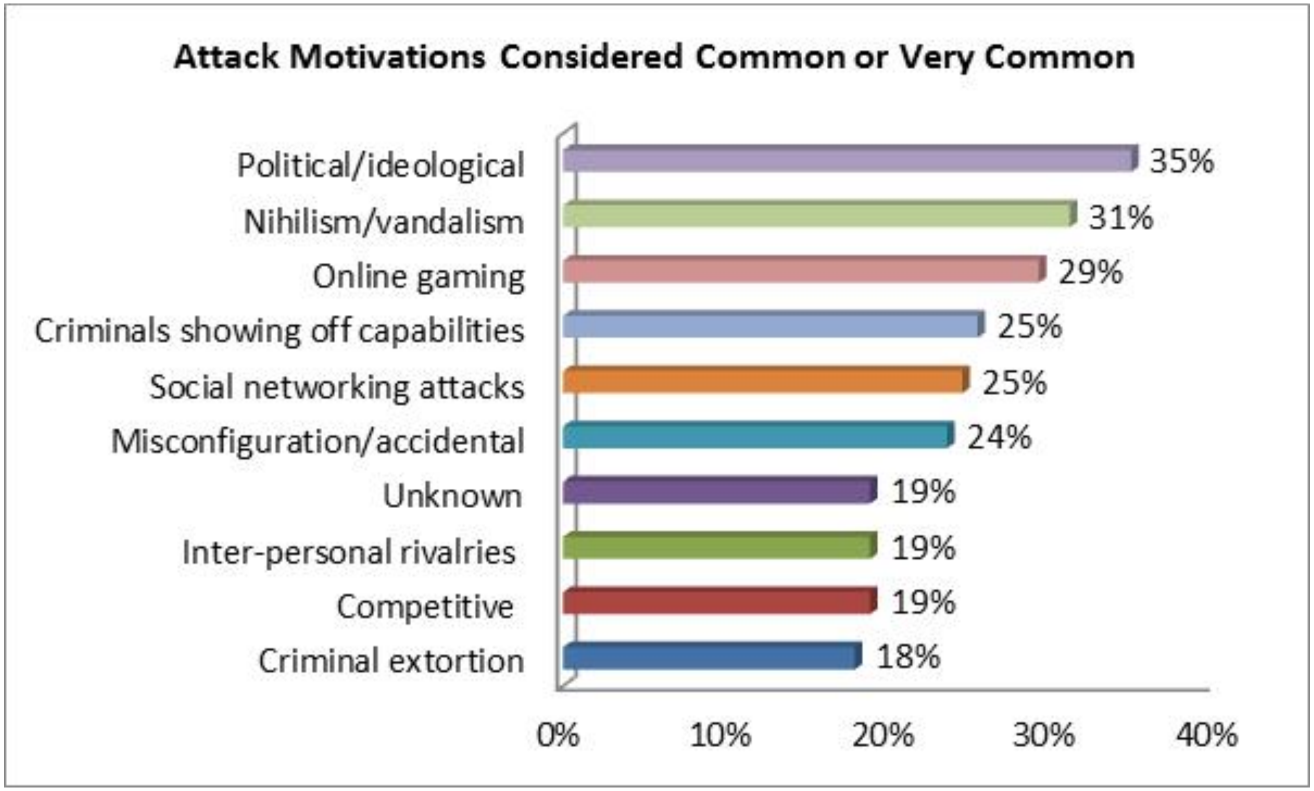
DDoS Attacks over the last 12 Months

DDoS Attack Frequency over last 12 Months



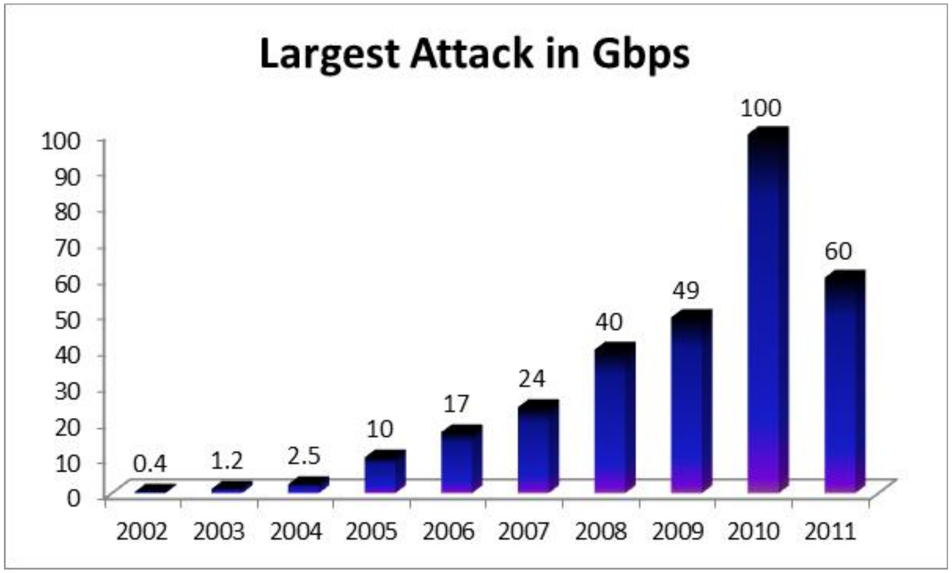
- **91% of respondents see at least 1 DDoS attack per month up from 76% in 2010**
- **44% of respondents see 10 or more attacks per month up from 35% in 2010**

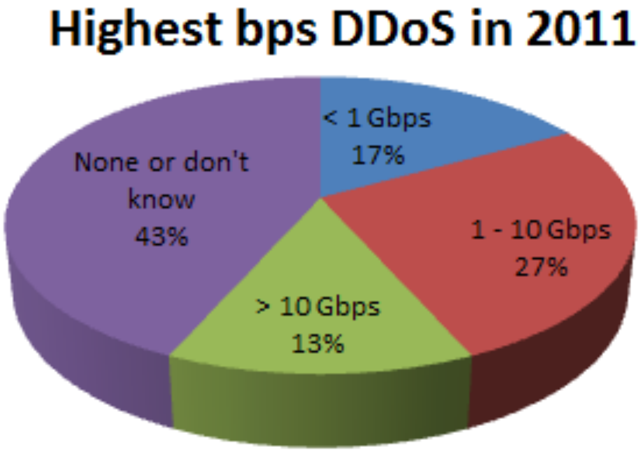
Top DDoS Motivations



- Top two attack motivation categories are fueled by personal beliefs and inclinations of attackers
- Exponential increase in risk of being attacked

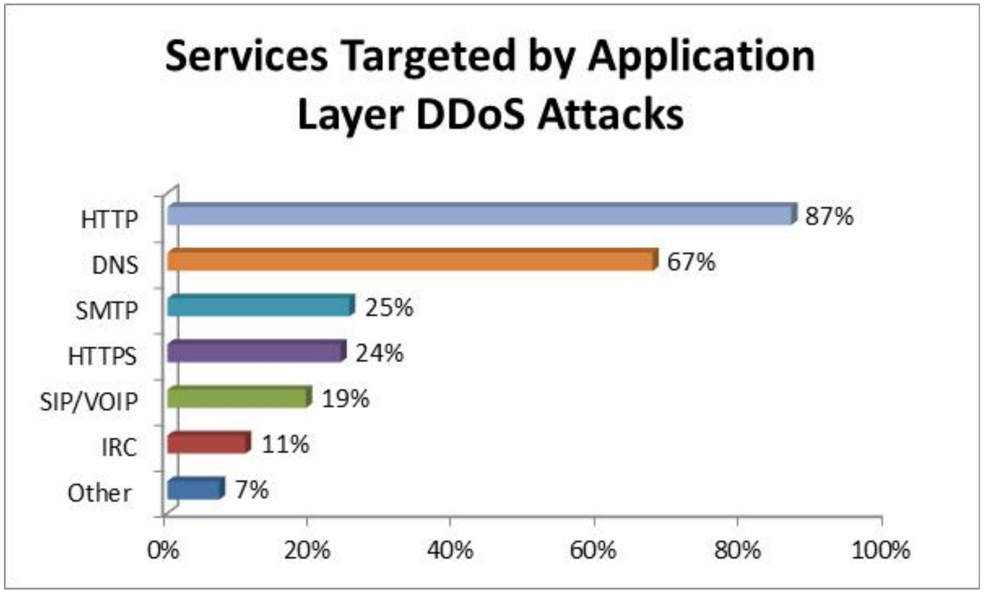
Large Attacks are Now Commonplace

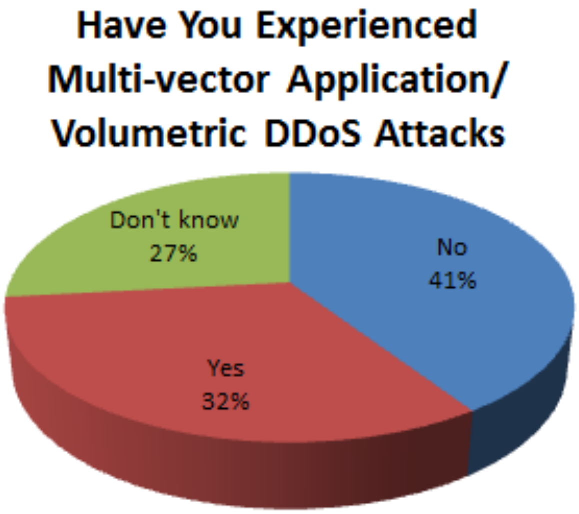




- Aggregate attack sizes have leveled off but remain at levels capable of overwhelming most Internet operators
- 13% of respondents report attacks above 10 Gbps
- 40% of respondents report attacks above 1 Gbps
- Largest pps attack reported is 35 Mpps keeping pace with 2010

Application Layer and Multi-vector DDoS



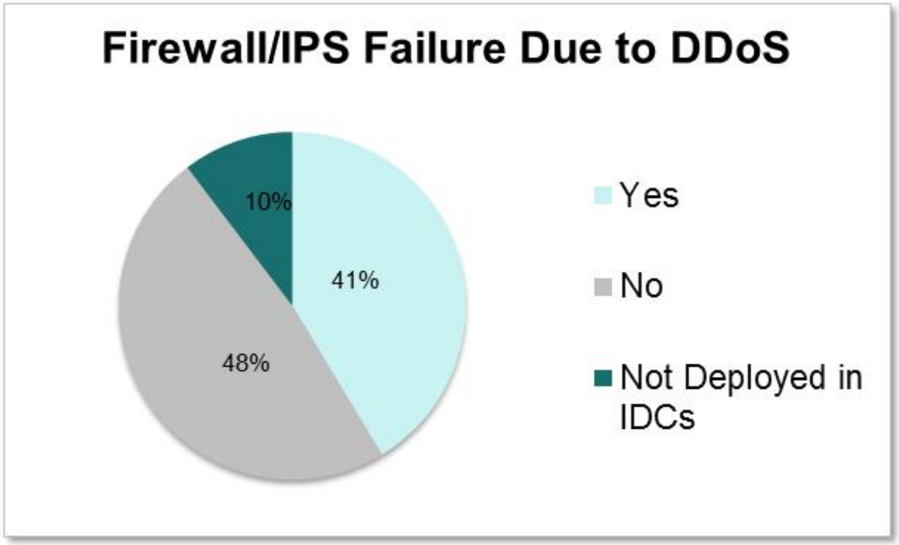


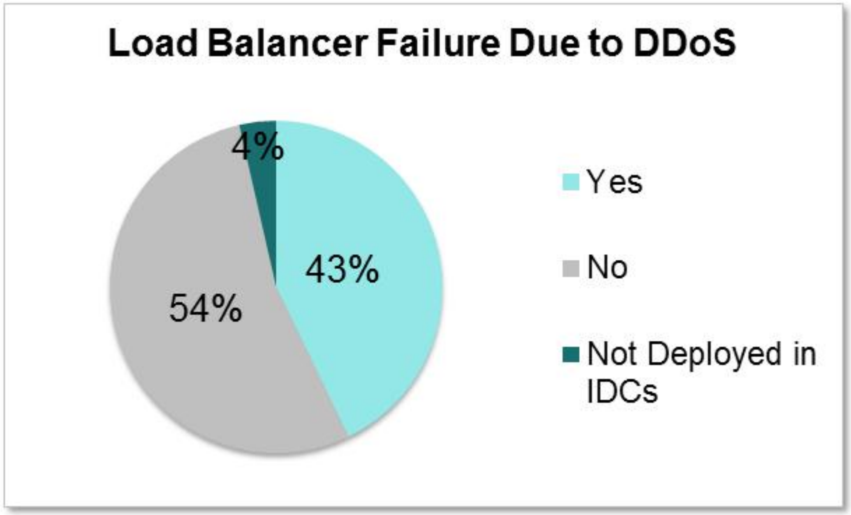
- **A higher percentage of attacks reported on HTTP and IRC relative to 2010**
  - HTTP (87% vs 84%) and on IRC (11% vs 0%) relative to 2010
- **Lower percent of attacks on DNS, SMTP, HTTPS and VOIP**
  - DNS (67% vs 76%), SMTP (25% vs 40%), HTTPS (24% vs 35%) and VOIP (19% vs 38%)
- **SSL based attacks reported included TCP and UDP floods against port 443, port scanning attempts and Slowloris**

ARBOR® NETWORKS

Fragility of Stateful Devices in the IDC

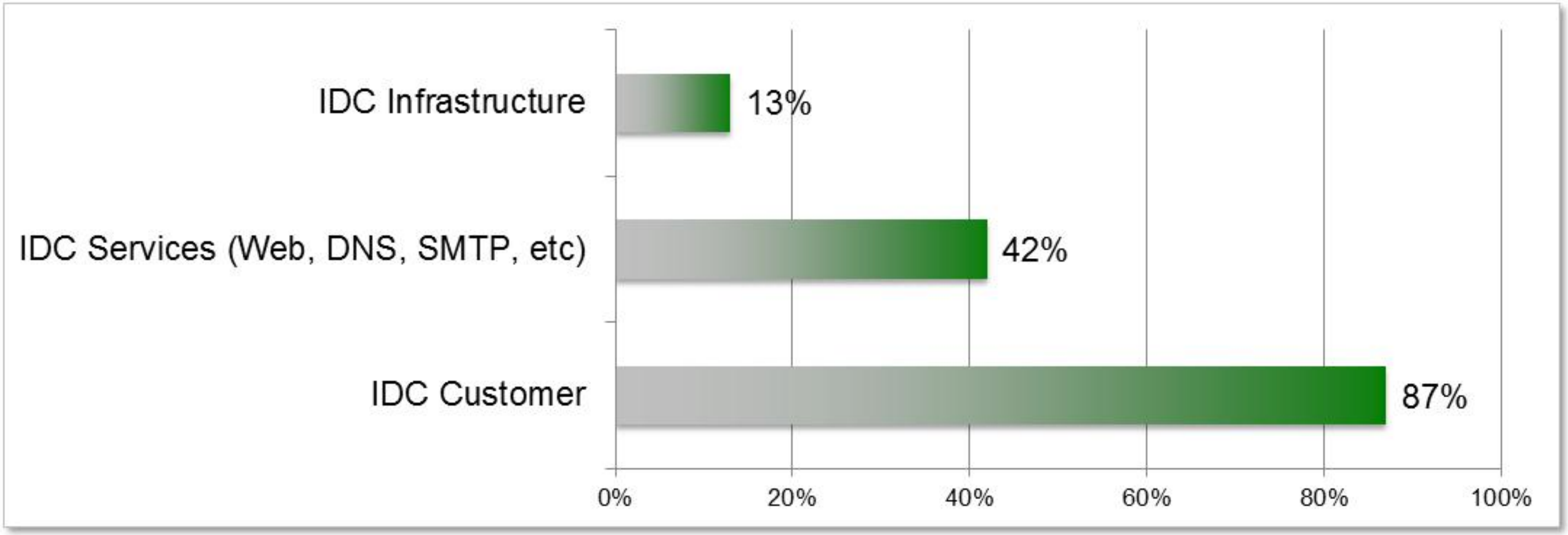
- Over 40% of respondents reported an inline firewall and/or IPS failing due to a DDoS attack.
- This is slightly lower number than 2010
  - May be due to increased deployment of mitigation devices protecting firewalls





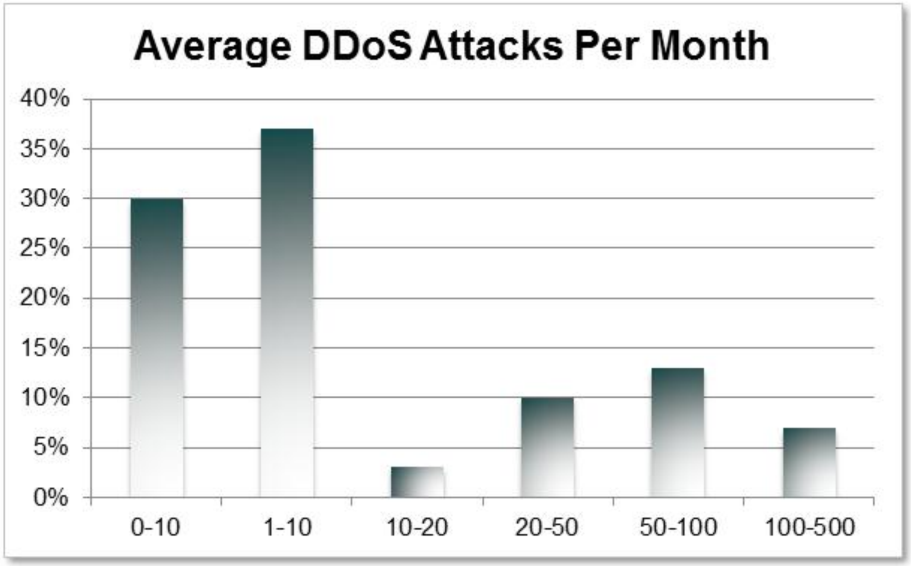
- 96% of respondents use load balancers within their IDCs
- 43% of respondents reported a stateful Load Balancer (or ADC) going down due to a DDoS attack

Primary Targets of DDoS Attacks in IDC



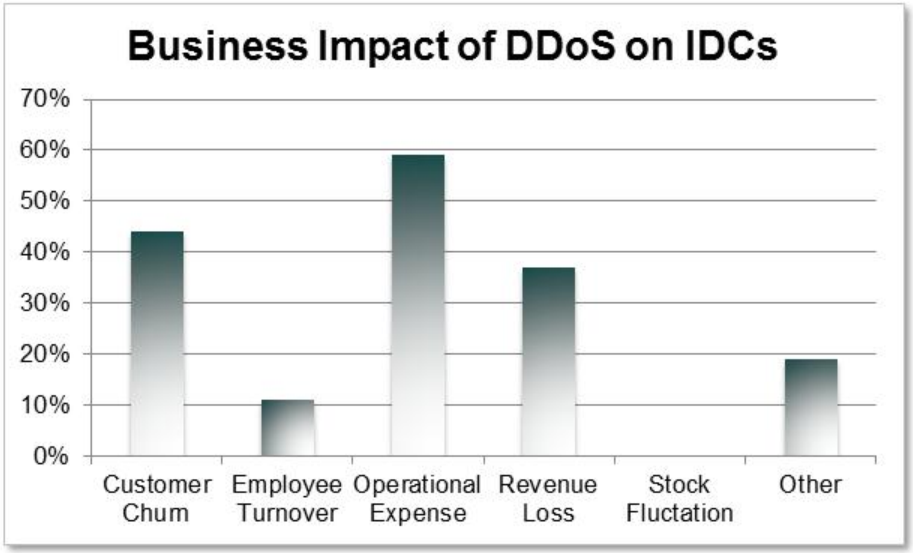
- Miscreant attacks against IDCs are generally focused on a specific customer
- In previous years, the attacks were equally against IDC services and IDC customers. In 2011, the attacks were targeted primarily against specific customers.
- IDC infrastructure is usually not the target of attacks.

Impact of DDoS Attacks on IDCs



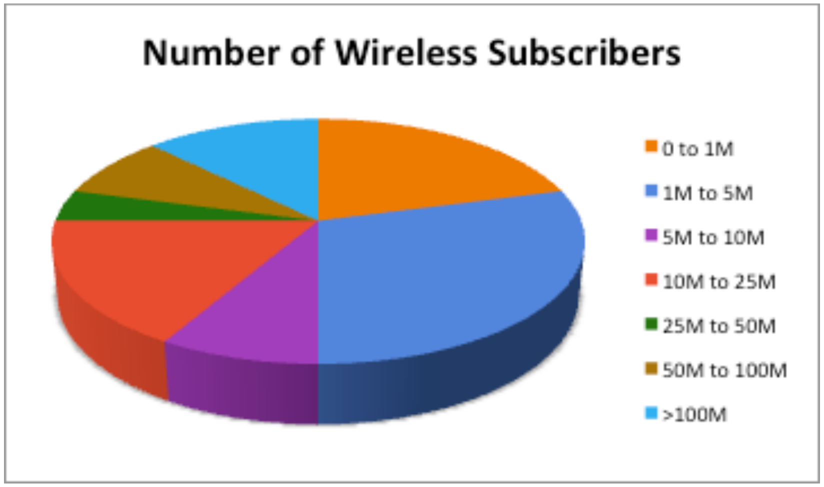
- 20% of respondents see over 50 attacks per month
- In 2010, only 15% of respondents experienced over 50 attacks per month

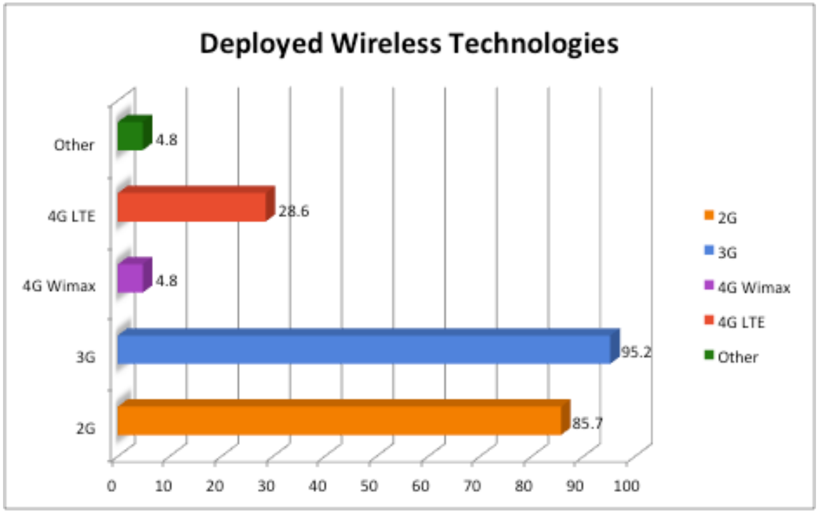
- Operational expenses continues to be the #1 business impact from DDoS in IDCs – it increased from 50% to 60% in 2011
- Direct revenue loss and customer churn also increased in 2011



Mobile Security

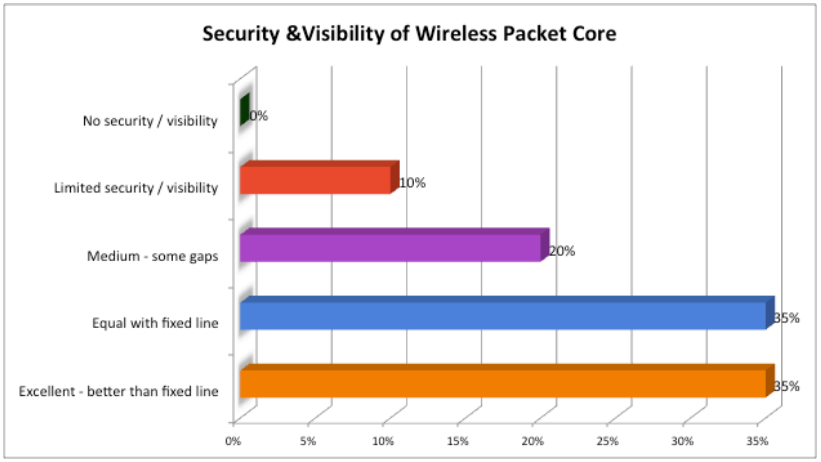
Mobile Services are Pushing Technology Adoption





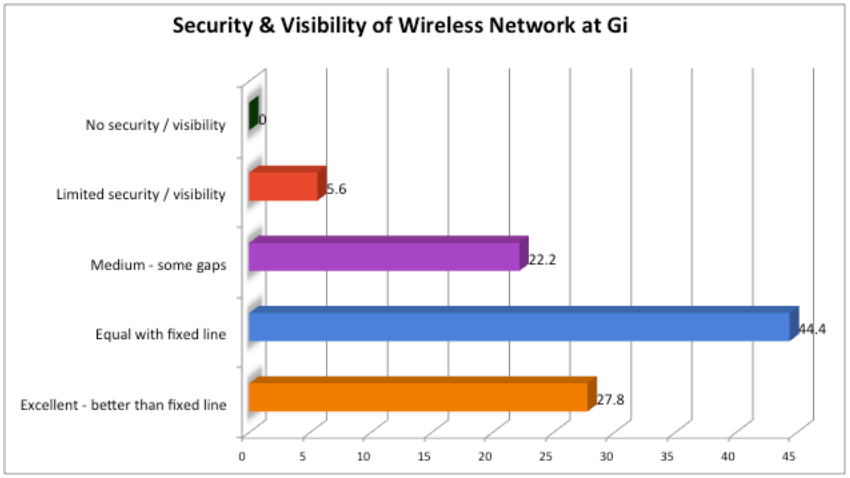
- **27% of survey respondents offered mobile services**
  - Ranging from 1M to over 100M subs
  - Range of subs shifted up, reflecting growth in Mobile
- **LTE availability accelerating**
  - LTE offered by 28.6%, up from 9% last year
  - Another 52% plan to have LTE deployed by 2014
- **IPv6 goes ahead**
  - 50% plan to introduce IPv6 within next 12 months.
  - 9.6% already have it.

Mobile Providers Investing in Visibility

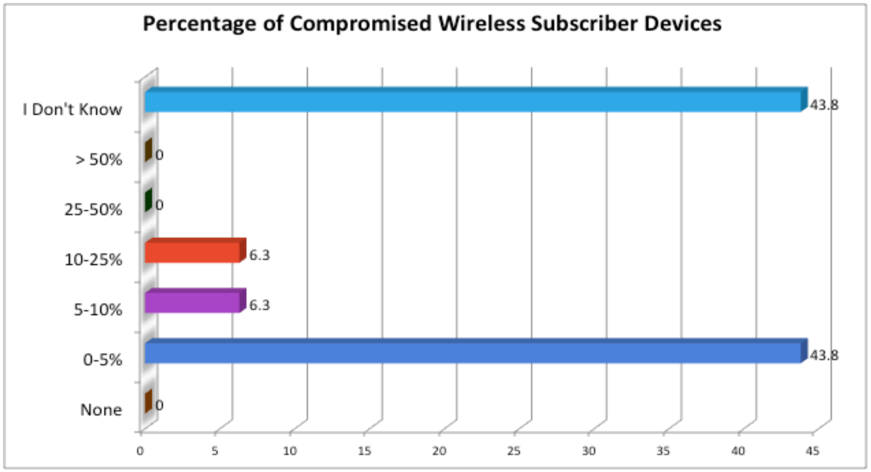


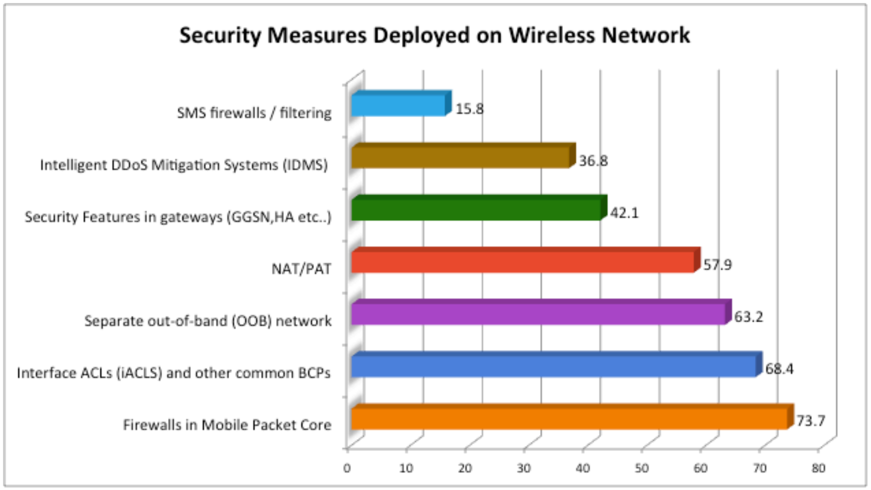
- **Big swing in traffic / threat visibility reported for the Mobile Packet Core:**
  - Only 10% now have limited visibility.
  - Down from 59% last year.
  - 35% have better visibility than on their fixed line networks.

- **And in traffic / threat visibility at the Gi:**
  - Only 6% now have limited visibility.
  - Down from 50% last year.
  - 28% have better visibility that on their fixed line networks.



Mobile Provider Subscriber Security Posture

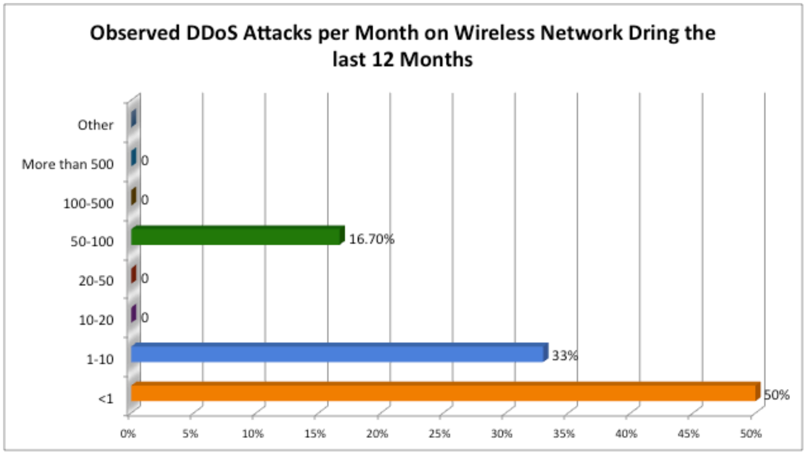

Percentage of Compromised Wireless Subscriber Devices

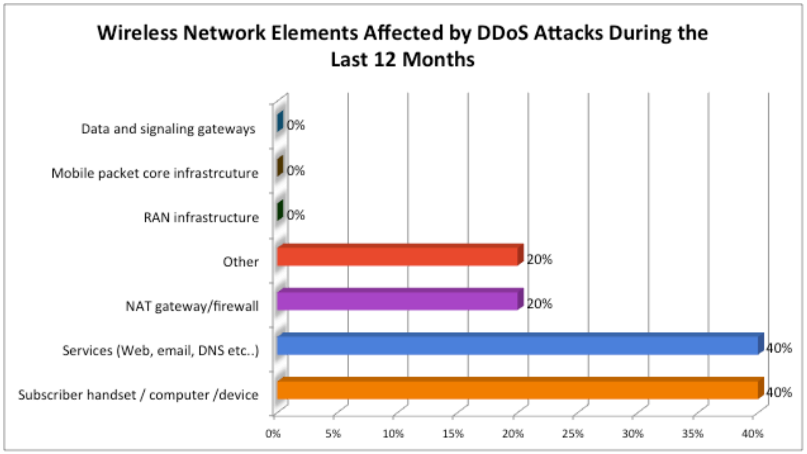

Security Measures Deployed on Wireless Network

- **Mobile respondents feel they have greater visibility into their network**
  - Swing from ‘none’ to 0-5% in percentage of compromised hosts
  - Operators know there is a growing problem
- **Firewalls lead the way for security with 74% of respondents using them**
- **Increase in use of other best practices such as iACLs, OOB management and IDMS**
  - 11.8% growth in the use of IDMS from 2010

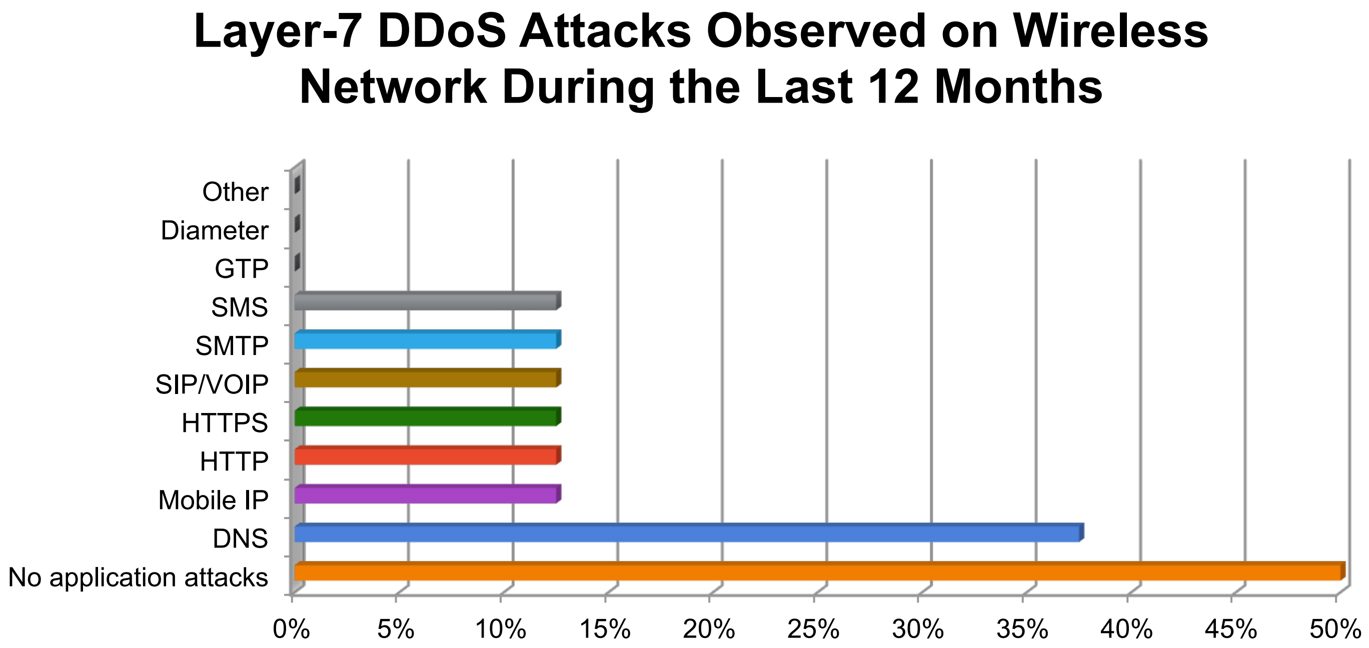
Mobile Infrastructure DDoS Attacks

- **50% are seeing attacks regularly**
  - 16.6% have seen outages due to DDoS
  - Big split in number of reported attacks per month
  - Attacks against mobile packet core and wireless infrastructure reported
- **Broad range of attack targets**
  - Subscribers & Services still top
  - NAT gateway lower than anecdotal information.
- **Outbound attacks down from 50% in 2010 to 36% in 2011**
  - 29% say they don't know
  - This shows that visibility down to the host level is not as good as it could be





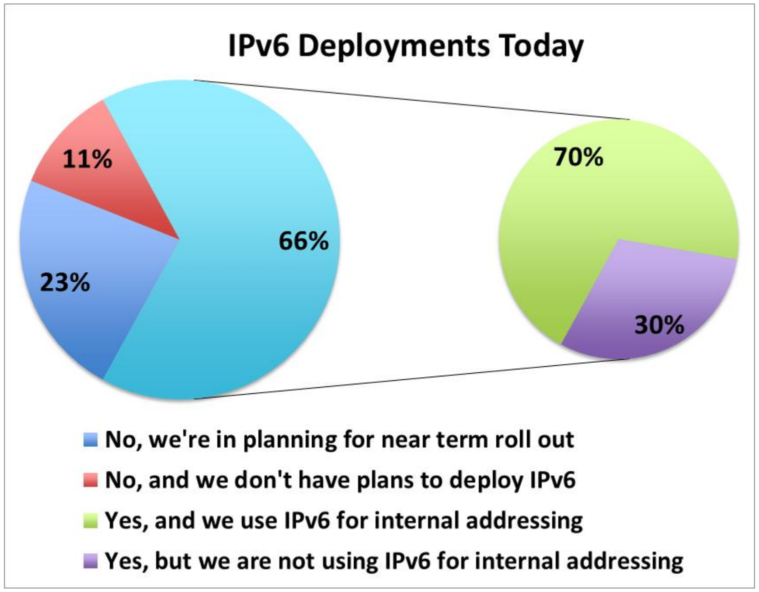
Mobile Infrastructure DDoS Attacks

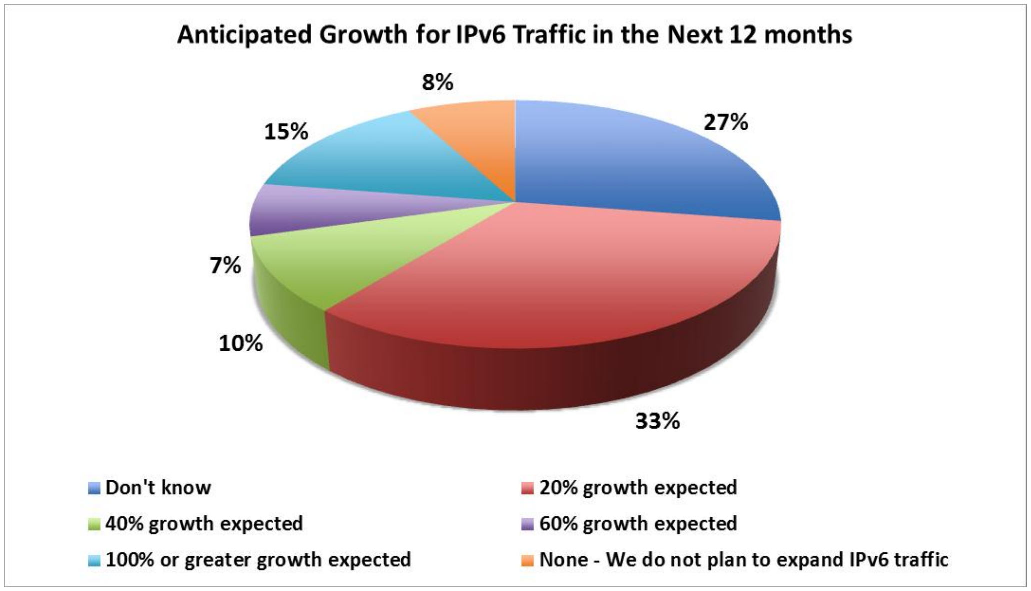


- **50% see application layer attacks on their networks**
  - Broad spread of attack types - similar to what we see elsewhere
  - DNS is the most common target – target with the most widespread damage potential
  - Surprise that HTTP was not top as last year, especially given general trends

IPv6

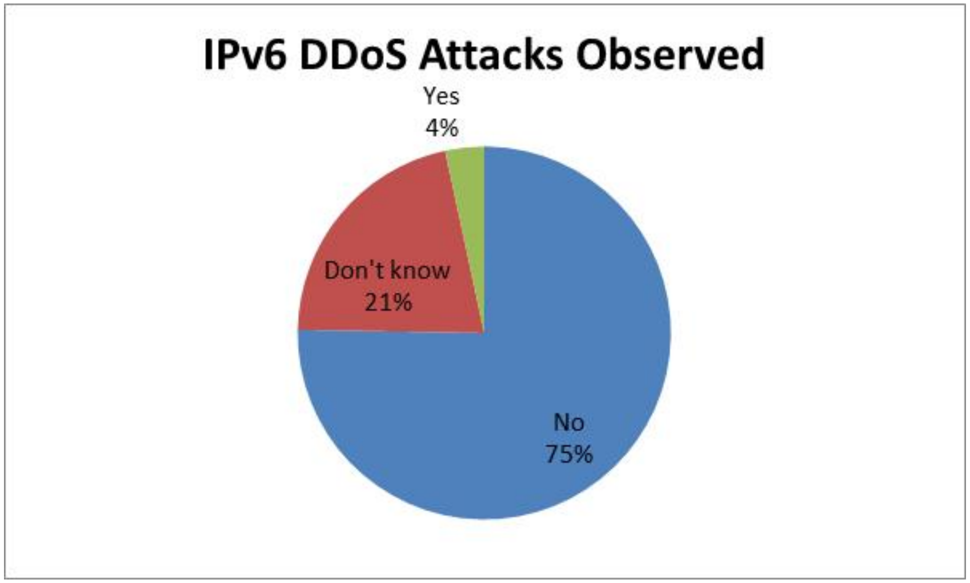
IPv6 Rollout and Growth





- **Two thirds of respondents have deployed IPv6 in their networks**
  - Majority of those who deployed IPv6 are using IPv6 for internal addressing of their network infrastructure
- **Two thirds of those who have not deployed IPv6 plan to do so in near term**
- **Traffic and volume remain low with varied forecasts for growth**
- **One respondent provided following answer indicating overall mood:**
  - *"depends of what youtube and company are doing ;)"*

IPv6 DDoS Attacks



- First report of an IPv6 DDoS attack in the history of the WISR
- Low frequency of attacks reflect low adoption of IPv6 for critical services

ARBOR®
NETWORKS

Thank You