ARBOR NETWORKS

2010 Infrastructure Security Report

Darren Anstee
EMEA Solutions Architect

6th Annual Edition

Introduction

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

- Leading provider of SP network threat detection / mitigation, traffic monitoring and reporting solutions.

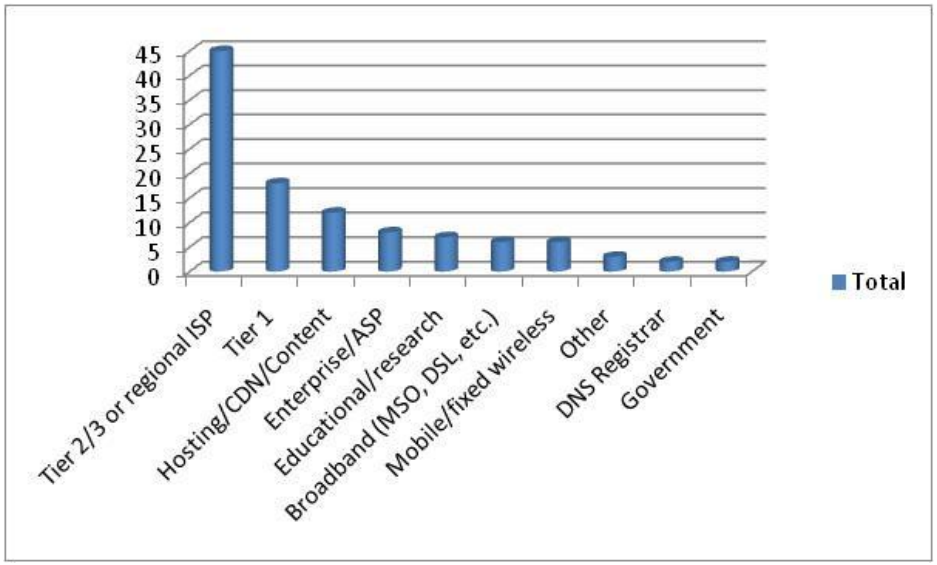
ARBOR® NETWORKS
How networks grow™

- 300+ employees in 20+ countries
- 300+ customers.
  - 90% Tier 1 Providers, 60% of Tier2
- Privileged relationships with majority of world's ISPs

ARBOR® NETWORKS

2010 Infrastructure Security Survey

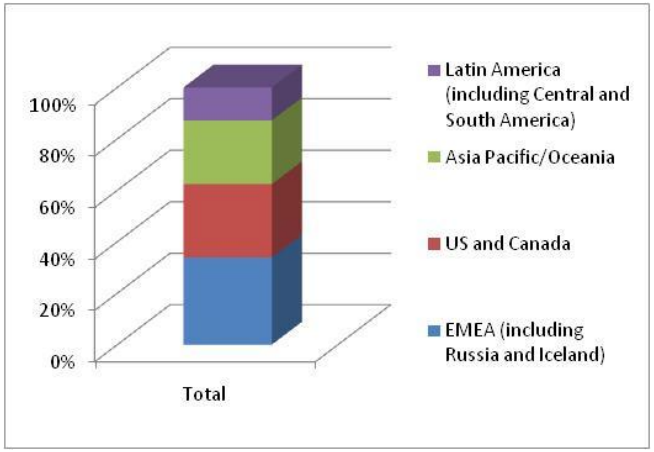
- **6th Annual Survey**
- **Survey conducted in September – October 2010**
- **111 total respondents contributed**
  - Service providers
  - Content/ASPs
  - Enterprises
  - Broadband
  - Mobile
  - DNS
  - Educational

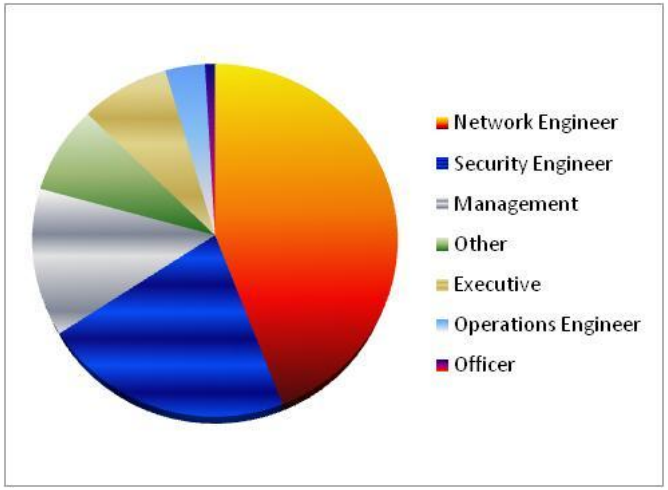


ARBOR NETWORKS

Survey Demographics

- **57% are service providers**
- **Even geographic distribution**
  - 34% EMEA
  - 28% US and Canada
  - 25% APAC
  - 11% Latin America
- **Tier 1 participation jumped to 15% of the respondents from 5% in 2009**
- **69% of respondents network, security or operations engineers**
- **22% of respondents were management or executives**





ARBOR NETWORKS

Key Findings of the Survey

- **Threat severity and complexity continue to increase**
  - Attack size increases dramatically, impacting underlying network infrastructure
    - 102% increase in attack size YOY
    - Broke 100Gbps barrier for first time
    - Up 1000% since first Arbor's first WISR in 2005
  - Application layer attacks continue with some new applications being targeted more frequently.
    - HTTP and DNS remain the top targets but HTTPS, SMTP and SIP/VOIP attacks are becoming more common
  - **The Threat-to-Defense gap is the widest observed to date**
  - DDoS attack capabilities of miscreants are outpacing the defensive measures taken by network service providers
- **Firewall and IPS equipment represents critical points of failure during DDoS attacks**
  - These products are commonly the targets of DDoS attacks

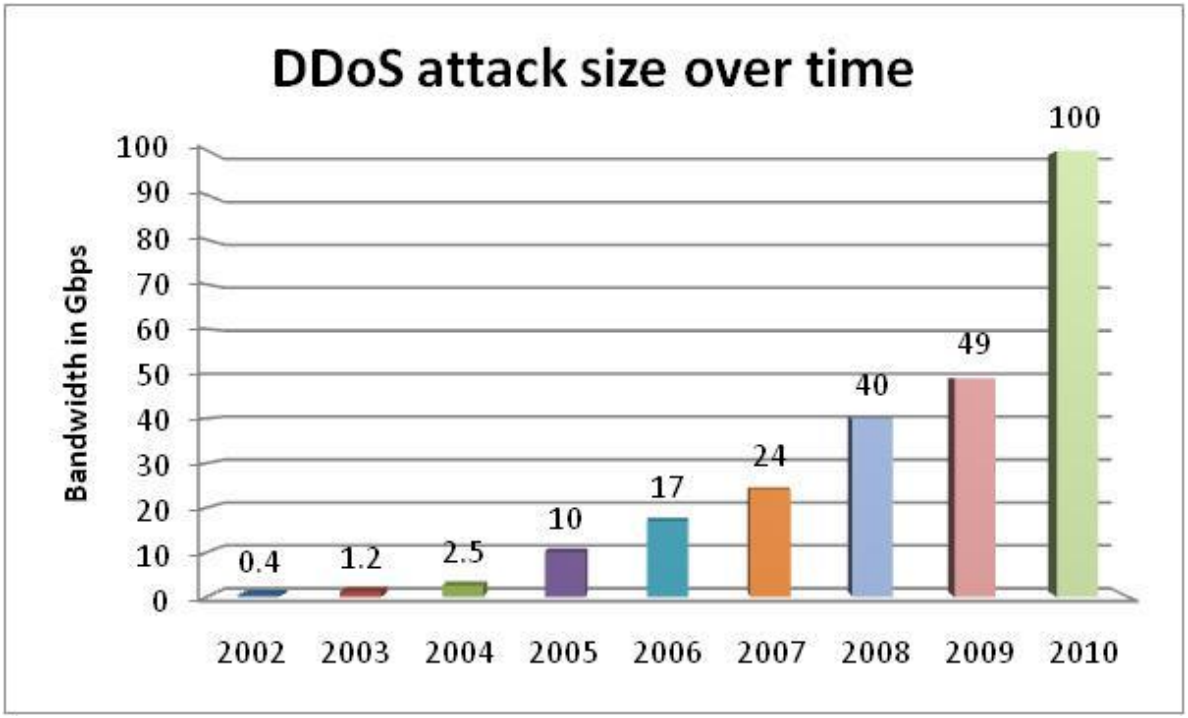
ARBOR NETWORKS

Key Findings

- **Mobile network growth is a game changer – availability of limitless botnets with greater bandwidth and few network control points**
  - 55% of mobile respondents have had outages in last year due to security incidents
  - In addition, over 50% admit that they have limited visibility into their mobile network
  - Mobile operators security capabilities are a decade behind wireline networks
- **Fragility of Internet Infrastructure**
  - DNSSEC security concerns on the rise as deployments begin
  - IPv6 security has become an arms race

ARBOR NETWORKS

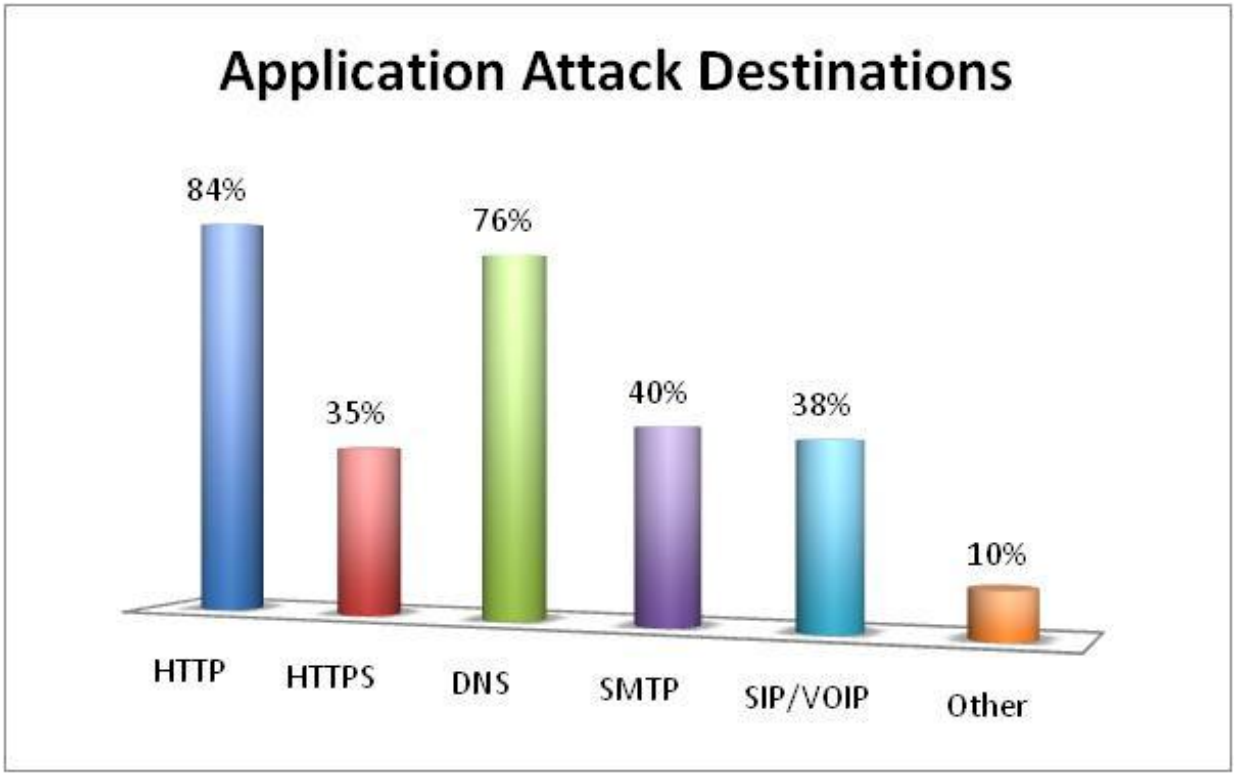
DDoS Attack Sizes Over Time



- **Over 102% increase YOY in attack size shows resurgence of brute force and volumetric attack techniques**
- **Internet providers have focused on application threats so miscreants turned back towards attacking network capacity**

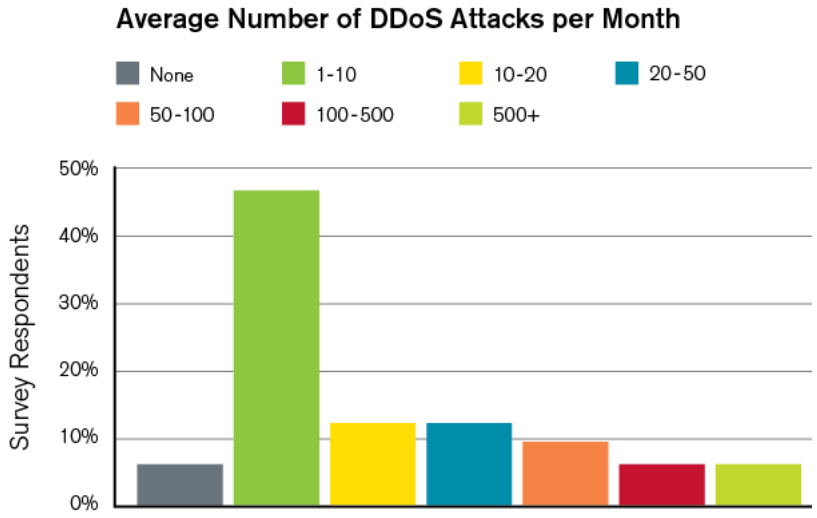
ARBOR NETWORKS

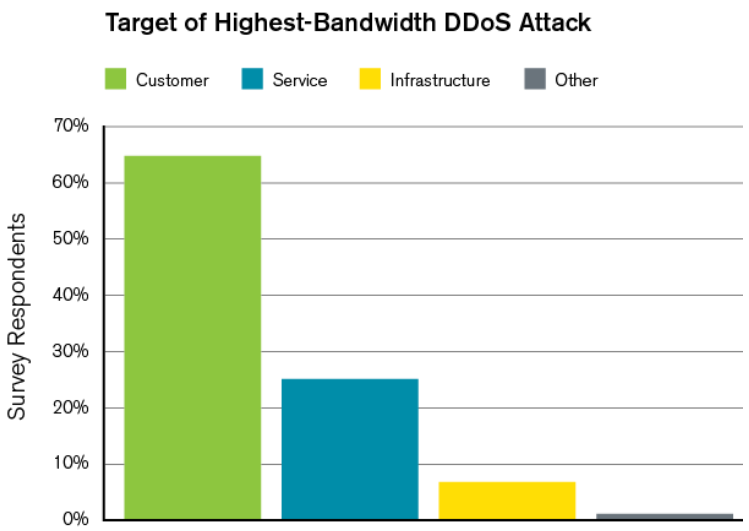
Application Layer Attacks



- **Application layer attacks are becoming common place**
  - 77% of respondents reported application layer attacks against critical services
  - Lynchpin service infrastructure remain top targets
  - Application attacks are advancing to more sophisticated services

Attack Frequency and Targets

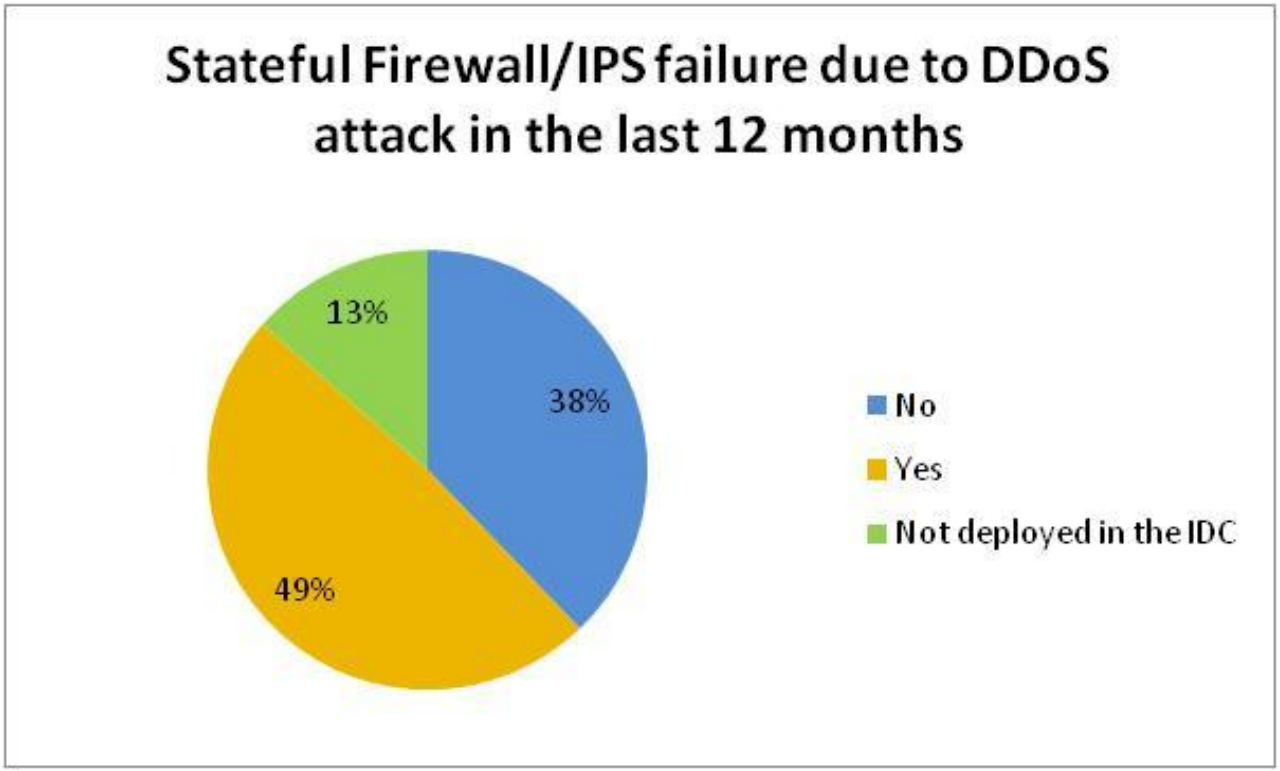




- **Attack frequency is increasing**
  - 94% of respondents see at least 1 DDoS attack per month
  - 35% of respondents see 10 or more DDoS attacks per month compared to 18% in 2009
- **Customers or services comprise 87% of targeted victims**
  - Major collateral events are less common, but drive greater impact

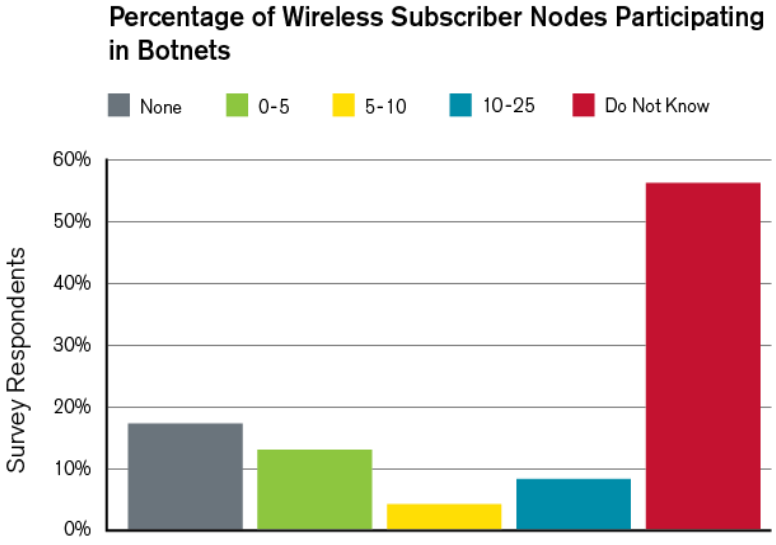
ARBOR NETWORKS

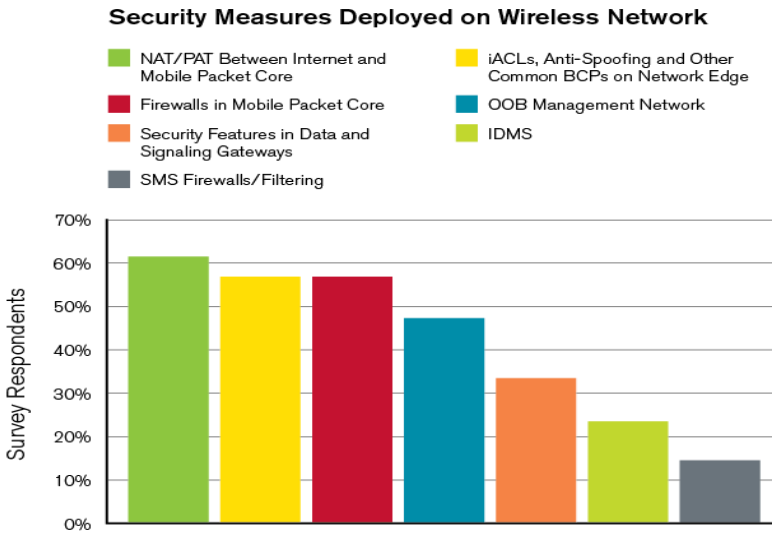
Failure of Firewall and IPS in the IDC



- **Nearly half of all respondents have experienced a failure of their firewalls or IPS due to DDoS attack**

Mobile Provider Security Posture



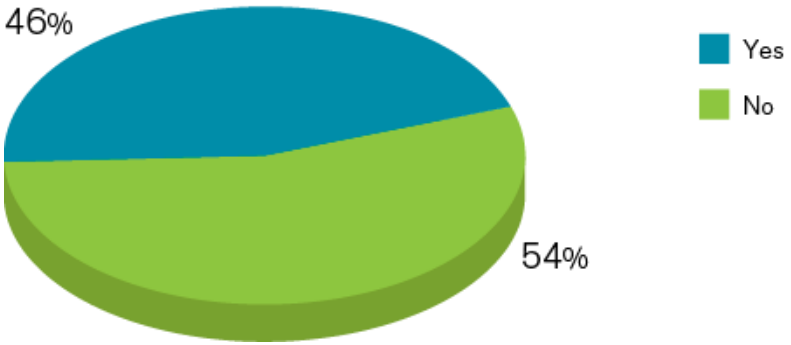


- **Roughly 50% report security problems with mobile subscribers**
- **Mobile respondents demonstrate poor visibility into compromised hosts**
  - 56% have no visibility into scale of compromised handsets
  - Optimistically, 17% say that there are none in the network
  - And 13% operators say at least 5% of customer base is compromised
- **Majority use NAT, firewalls and ACLS**
  - 47 to 60%
- **DDoS mitigation and SMS filtering less common**

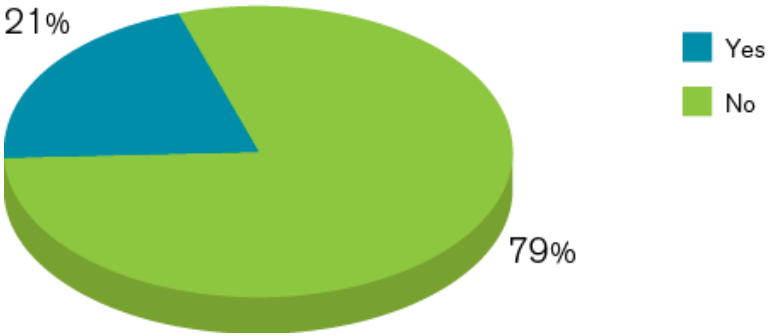
ARBOR NETWORKS

Mobile Security Incidents

Security Incidents Leading to Customer Outages



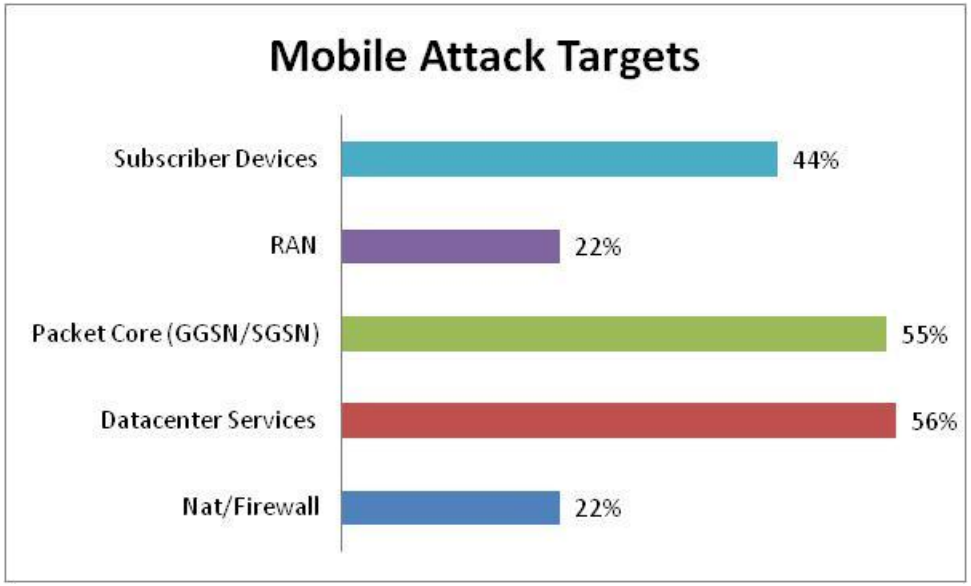
Attacks Explicitly Targeting Wireless Network Infrastructure

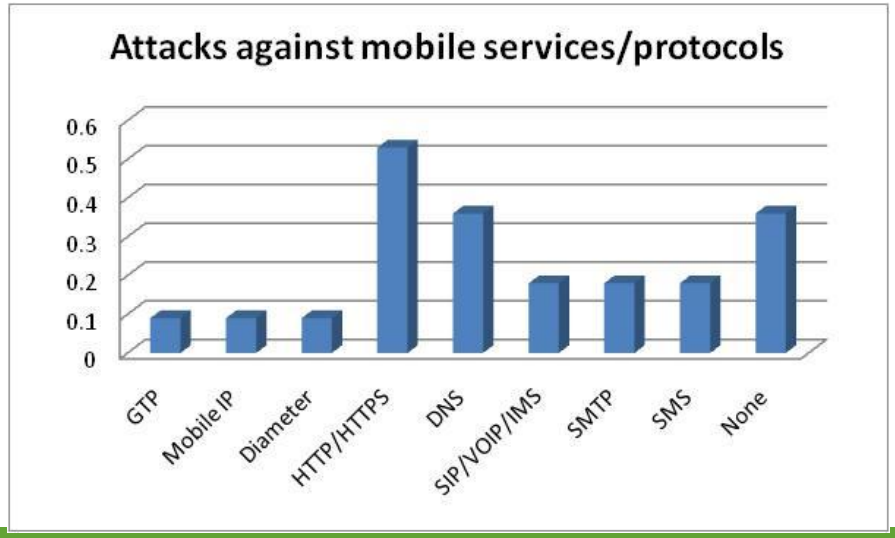


- **Nearly half of carriers have had outages in last year due to security incidents!**
- **79% of mobile respondents say that they have not had a DDoS event in the last 12 months but over 50% admit that they have limited visibility into their mobile network**
  - How many DDoS events are they having that they simply don't know about?
- **Mobile operators are more concerned about DNS, AAA, Mail attacks than fixed line providers**
  - 70% compared to 58% in fixed line

ARBOR NETWORKS

Mobile Infrastructure Attack Targets

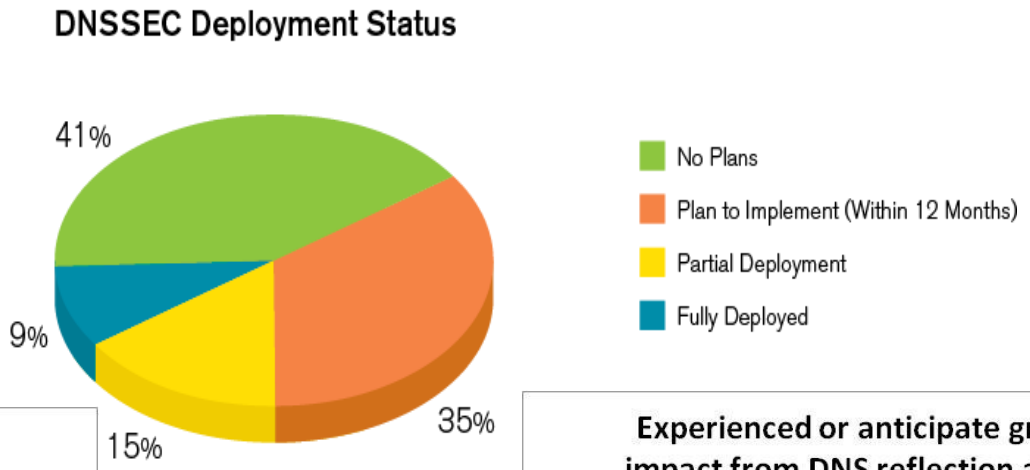


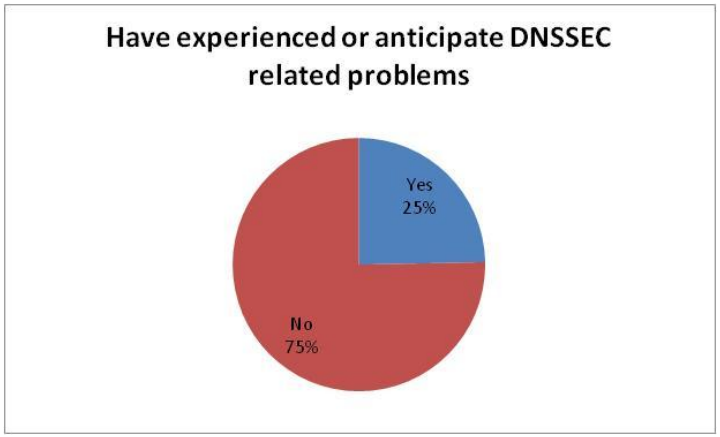


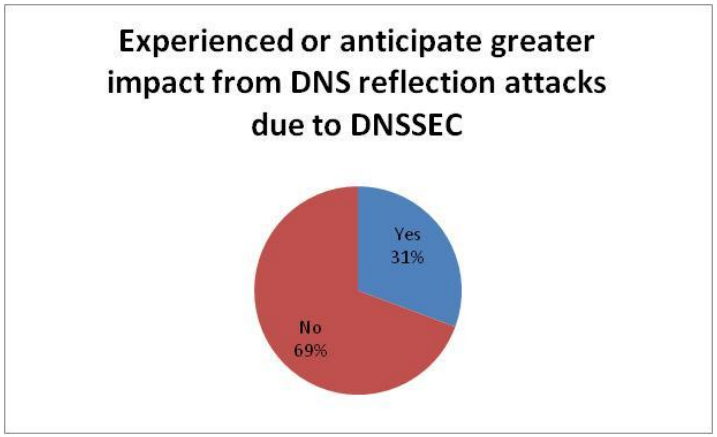
- **Broad range of attack targets within mobile network**
  - 56% attacks against packet core or mobile datacenter (DNS, web)
  - Attacks against subscriber devices next at 44%
  - RAN / Firewall attacks less common at 22%
- **Services targeted**
  - http / https and DNS are most common with VOIP, SMTP and SMS also targeted

ARBOR NETWORKS

DNSSEC Threats



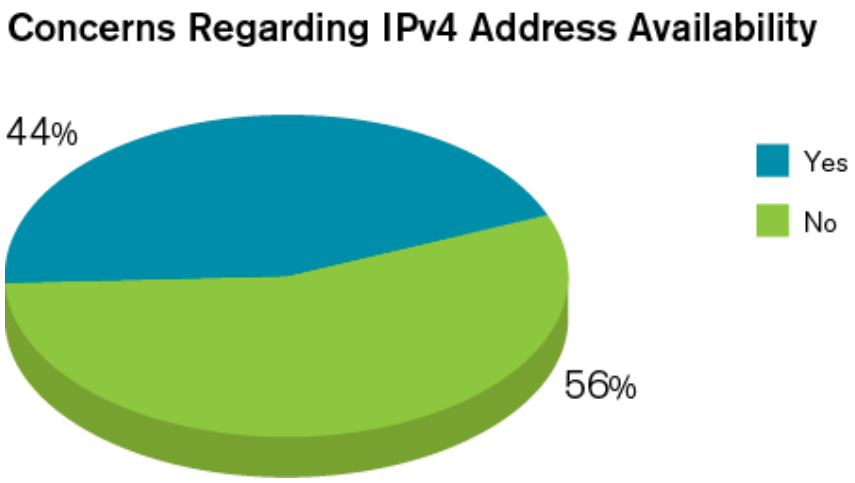




- 24% of respondents have deployed DNSSEC
- Already 25% have experienced or expect problems and 31% expect increase in amplification attacks

ARBOR NETWORKS

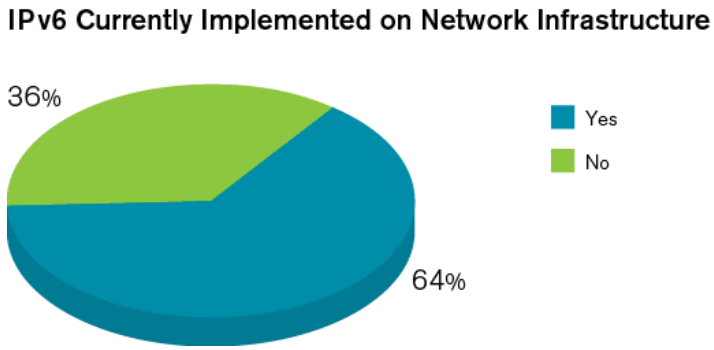
IPv4 Address Exhaustion

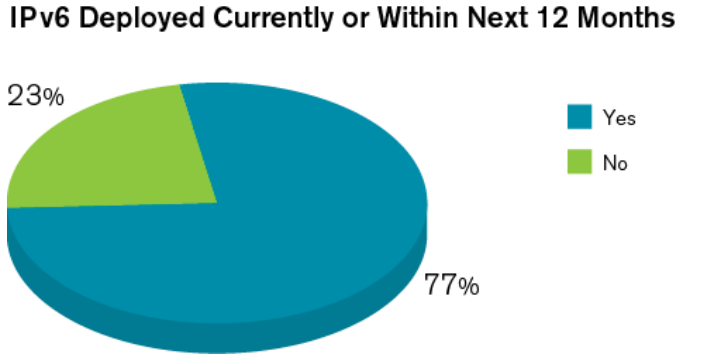


- 44% of participants predict that they will be exhausting their IPv4 allocations within the next 12 months
- With the overall industry exhaustion of IPv4 space, this may lead to business continuity concerns
  - Network architectures will need to be examined
  - More NAT/PAT use
  - Faster migration to IPv6

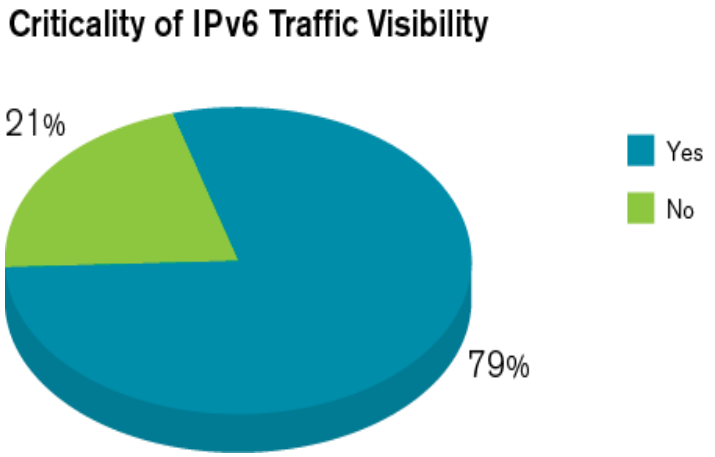
Deployed IPv6 is growing

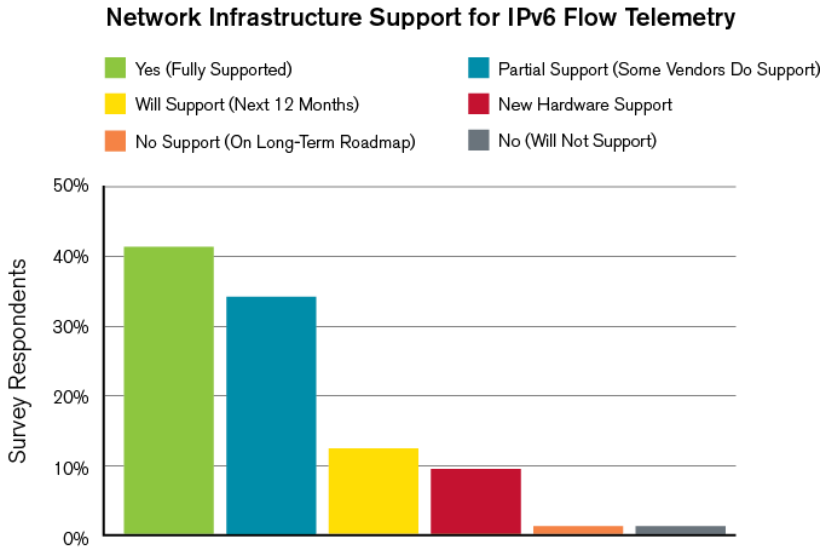
- 64% of respondents already have IPv6 deployed to a limited extent and 77% of respondents expect to have IPv6 deployed within 12 months
- 500Mbps is the peak today but major growth is expected with IPv4 address exhaustion
- Can security teams keep up?

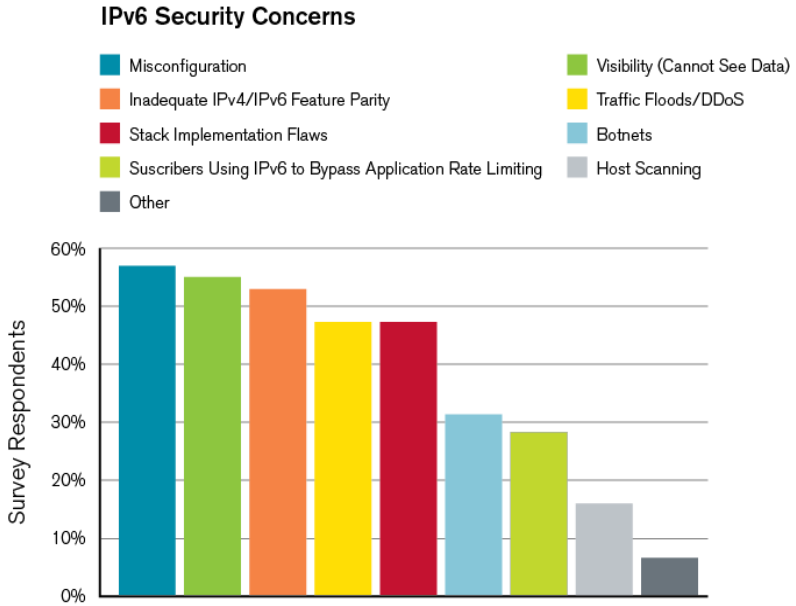




The IPv6 Security Arms Race



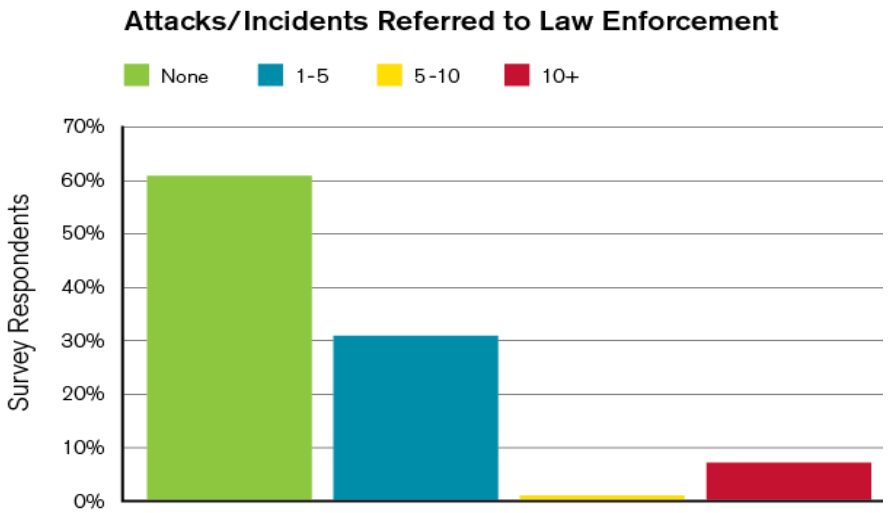


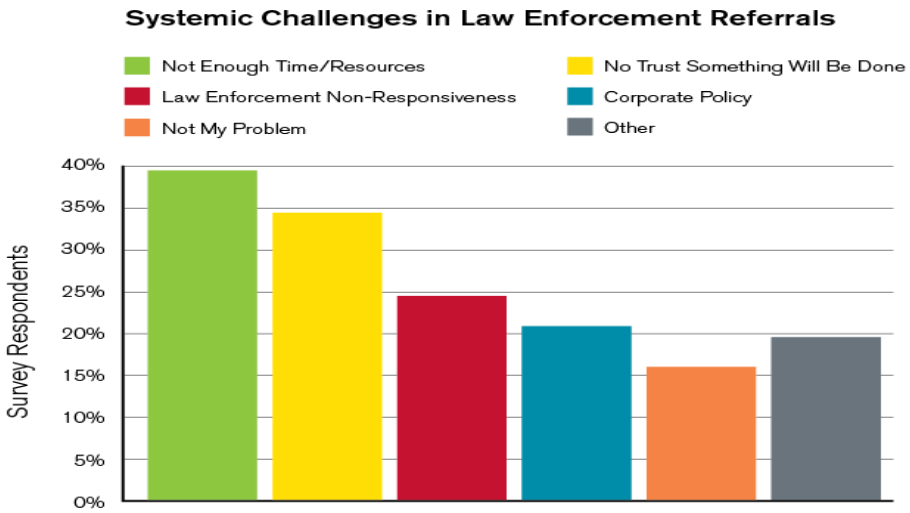


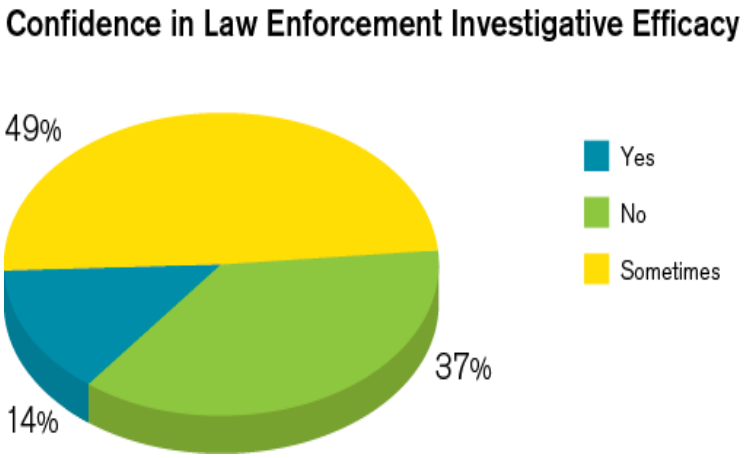
- **Vendors and network operators are rushing to introduce IPv6 visibility and security as networks scale up**

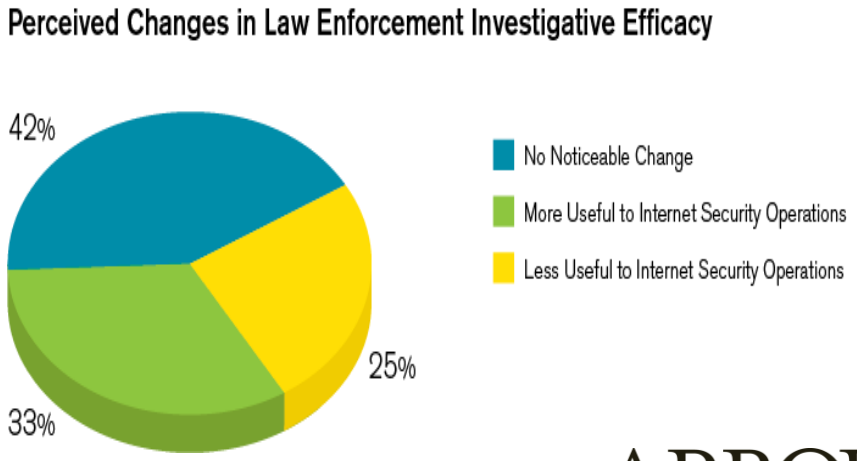
ARBOR NETWORKS

Confidence in Law Enforcement Remains Low









ARBOR NETWORKS

Thank You