

# **Fifth Annual Infrastructure Security Survey**

**Craig Labovitz**

**Roland Dobbins**

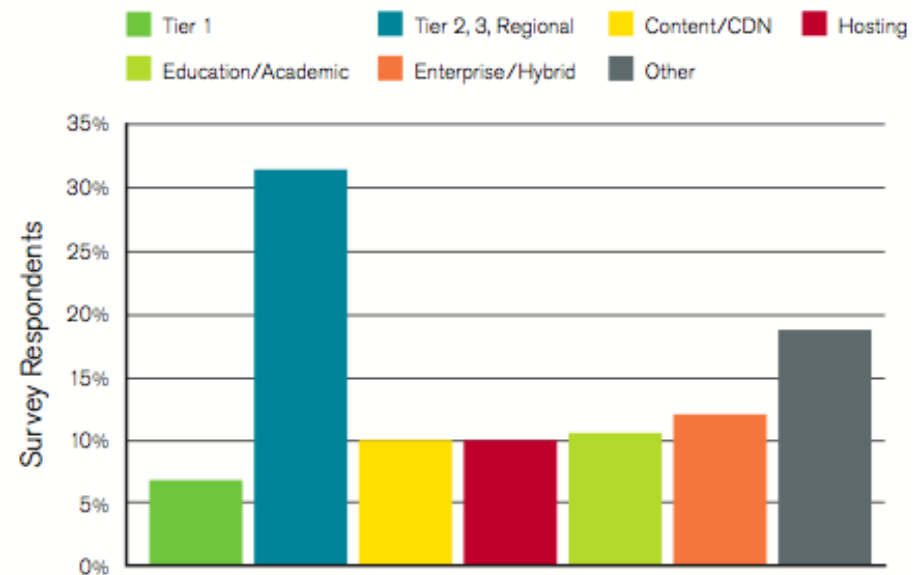
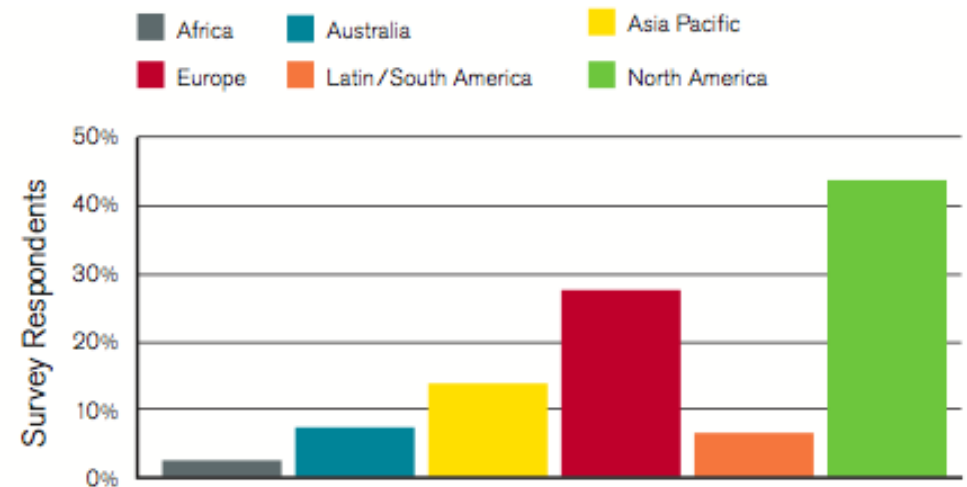
**Danny McPherson**

**Mike Hollyman**

Arbor Networks

# Survey Results 3Q 2008 – 3Q 2009

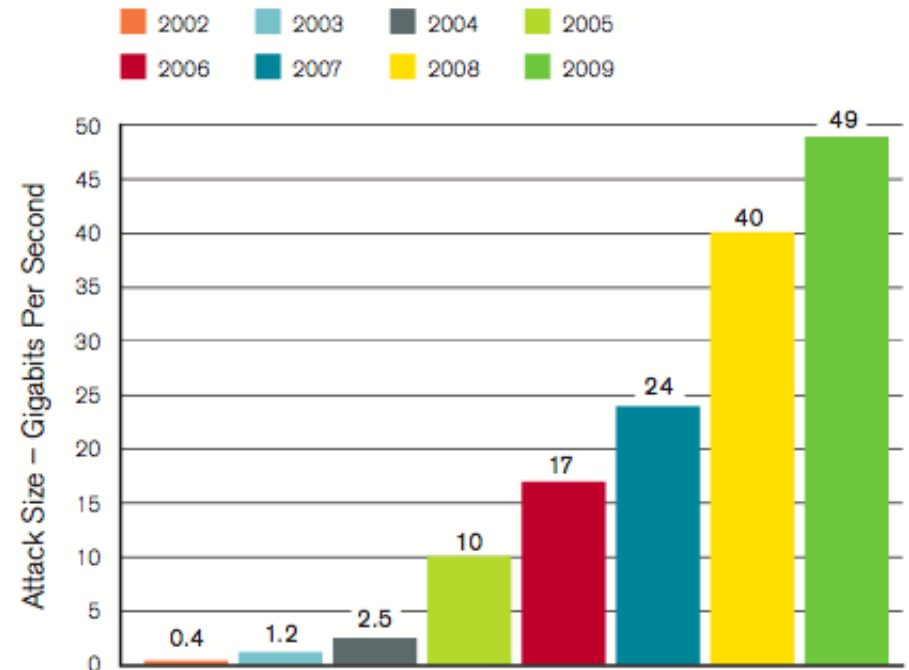
- 132 self-classified IP network providers
- *Double the participation vs. last year (66 respondents)*
- All participants are directly involved in network security operations.
- Major demographic shift away from self-described Tier 1 and Tier 2 providers towards Tier 2/3



# Good News: DDoS High Water Magnitude Slows?

- The largest attack reported 49 Gbps
- The largest sustained attacks reported were 40 Gbps and 24 Gbps, respectively
- However, DDoS attack scale growth has actually slowed over the past 12 months in comparison to previous years
- 2007-2008 Growth: 67%
- 2008-2009 Growth: 20%

**Largest DDoS Attack – 49 Gigabits Per Second**

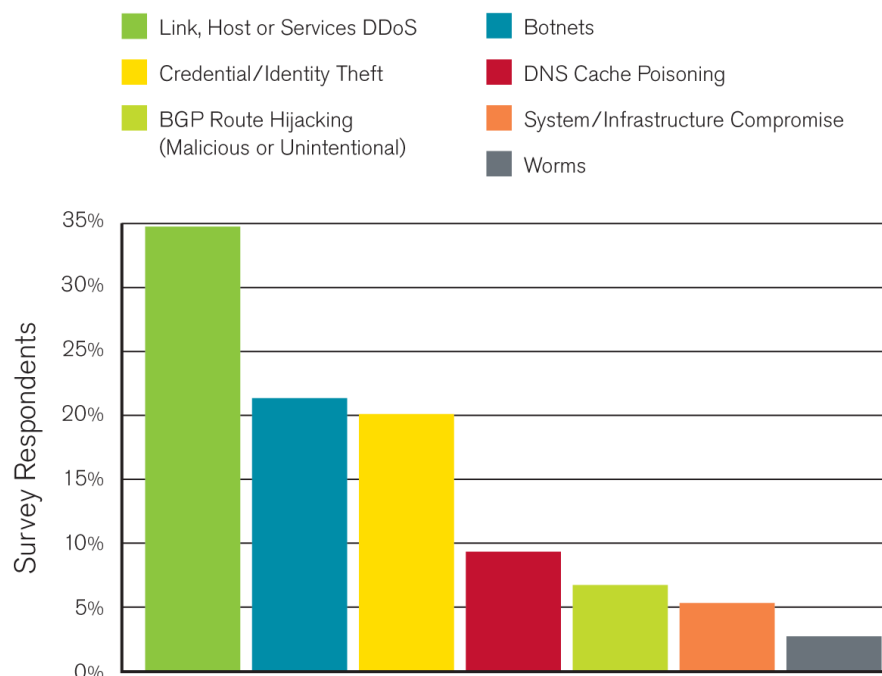


*Figure 1: Largest DDoS Attack – 49 Gigabits Per Second*

# What Scares Us?

- Multi-hour outages of prominent Internet services due to application-level attacks
- Significant threat to “Cloud Computing” adoption
- Designed to exploit service weakness
- Primary threat vectors for attacks targeting the cloud
  - ✓ Domain Name System (DNS) infrastructure
  - ✓ Load balancers
  - ✓ Large-scale SQL server back-end infrastructure

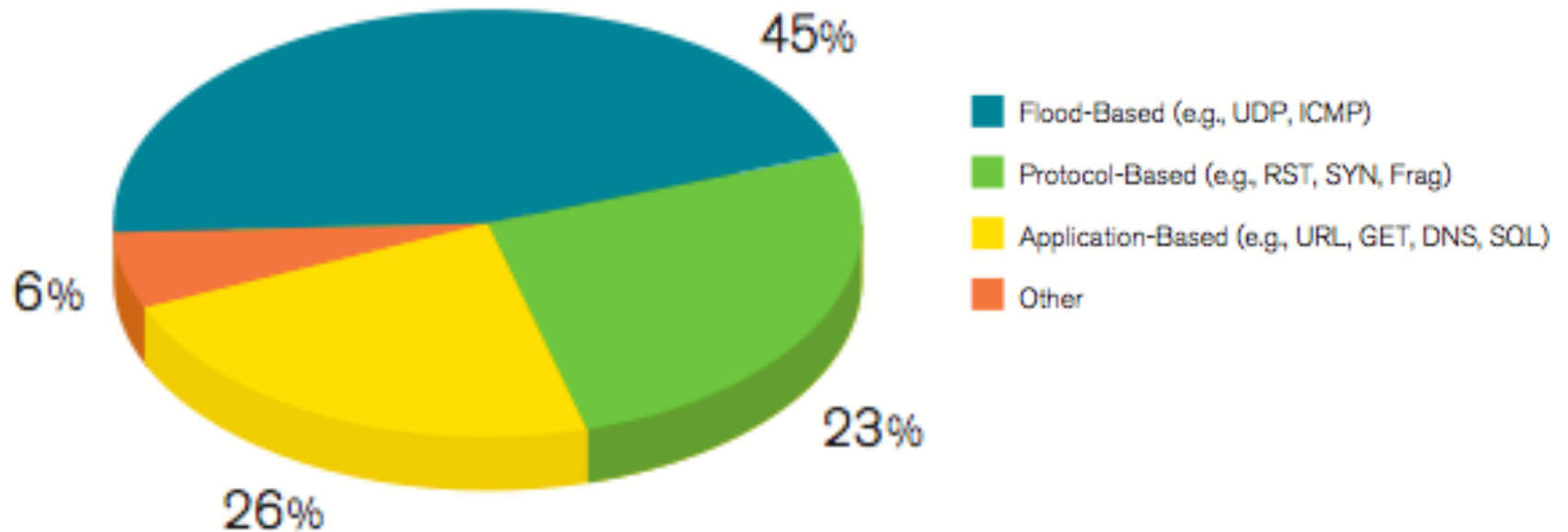
## Largest Anticipated Threat – Next 12 Months



# DDoS Attack Vectors

---

- Brute force attacks still dominate
- But growing number of service / application level attacks

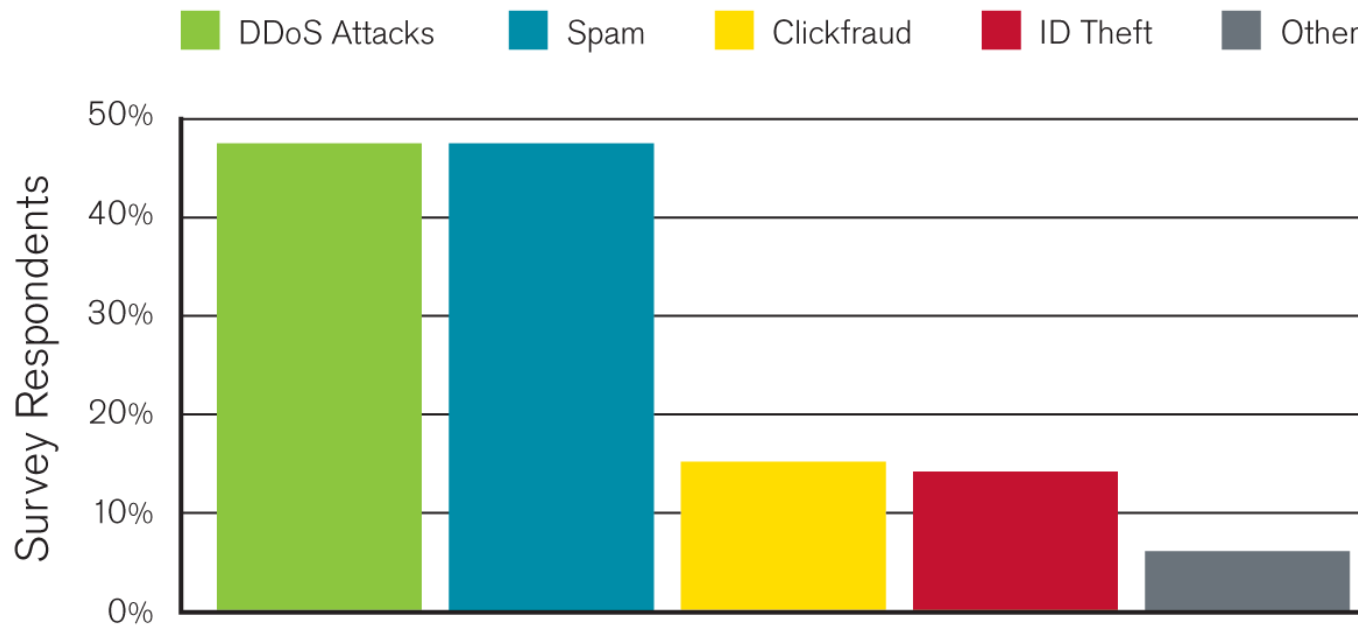


# Botnet Activity

---

- Not surprisingly, spam and DDoS share the top spot, for botnet-based activity

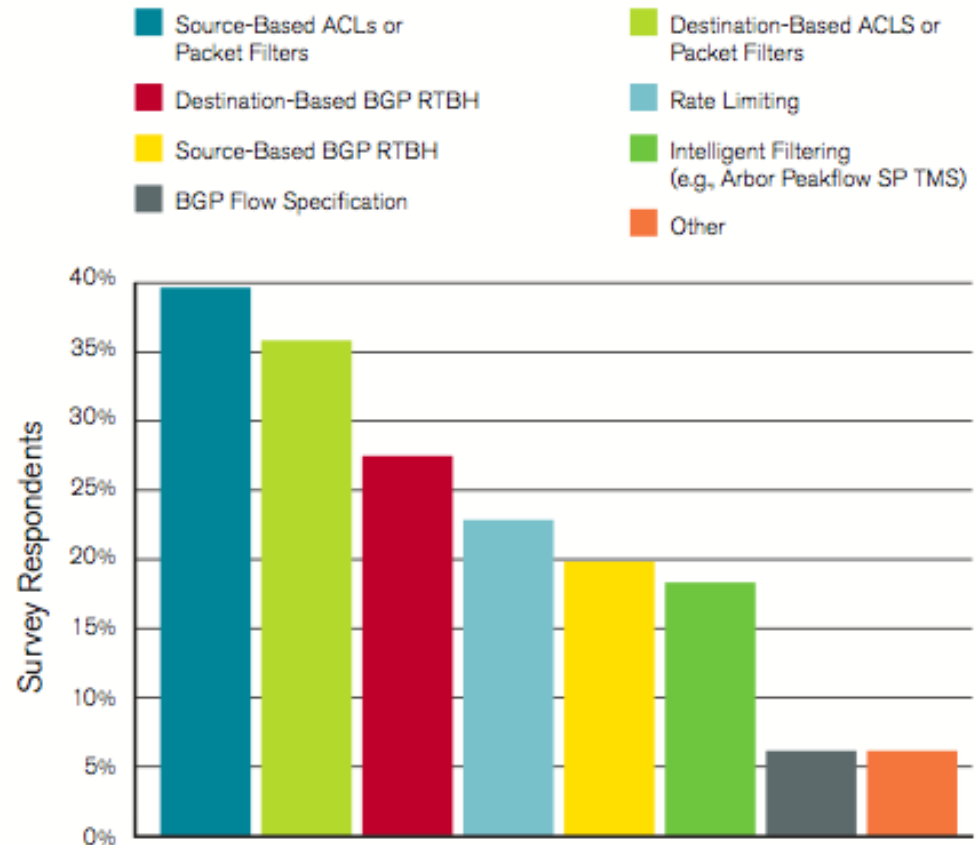
## Observed Bots – Past 12 Months



# Detection and Mitigation

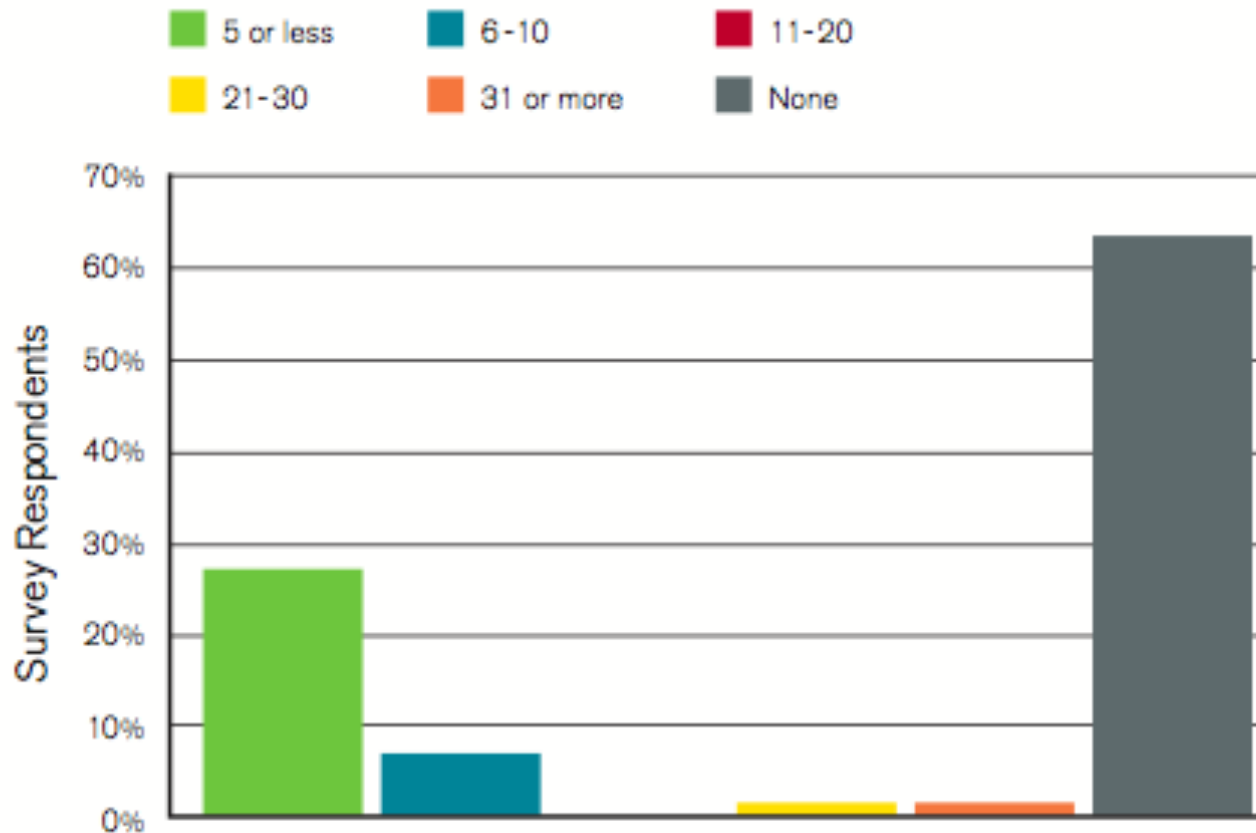
- Majority using ACLS
- Followed by BGP blackhole (src and dst)
- Intelligent filtering grew 14% to 18%
- And 58% using commercial detection tools (followed by customer calls at 35%)

## Primary Attack Mitigation Techniques



# Attacks Referred to Law Enforcement


- Still most attacks go unreported (95% said reported 5 attacks or fewer in last year)
- Jurisdiction, lack of confidence LEA, publicity





## Concerns: Vendor Security Support

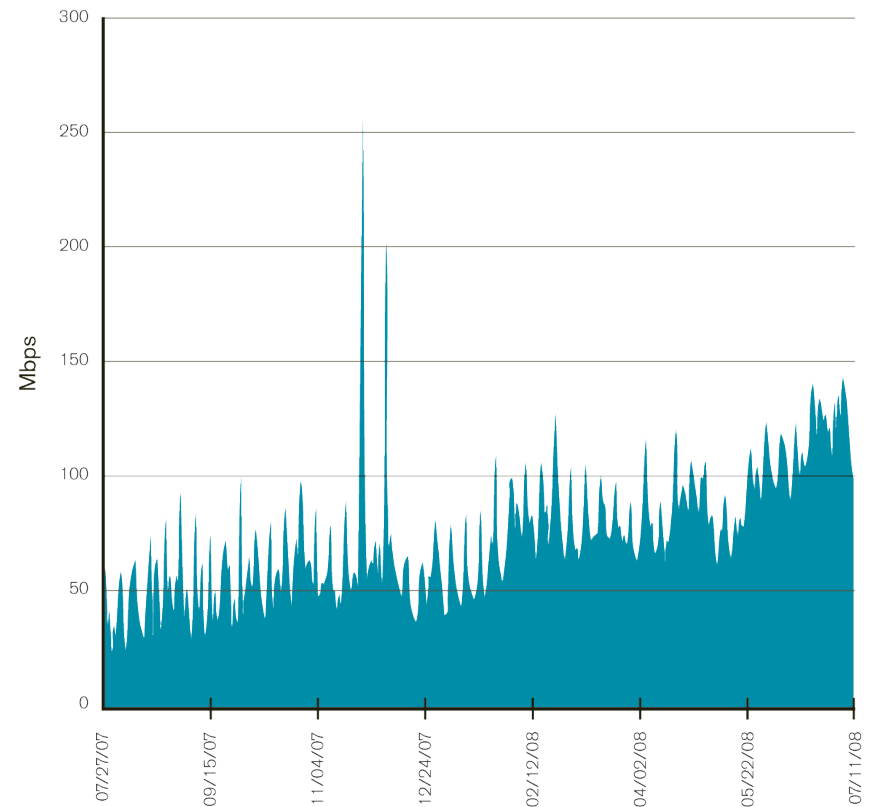
---

- **“Lack of feature/functionality parity and consistency across platforms.”**
  - **“Number and complexity of ACLs supported.”**
  - **“No sensible defaults for control- and management-plane self-protection.”**
  - **“Inadequate ACL performance at 10gb/sec and above.”**
  - **“IPv6 filtering and security capabilities.”**
  - **“Lack of hardware support for key features.”**
  - **“Lack of pps-based rate-limiting vs. bps-based rate-limiting.”**
  - **“High complexity, low usability.”**
  - **“Anything and everything to do with IPv6.”**
- 

# Concerns: The Internet is not IPv6 Ready

## Concerns:

- ✓ IPv6 is still viewed as unproven
- ✓ There is a lack of IPv6 tools and knowledge in operations
- ✓ IPv6 network infrastructure functionality lacks parity with IPv4,
- ✓ Management does not understand the need to invest in preparation for IPv6 interoperation and support



“Not many (any?) devices work on IPv6 the way they do on IPv4, especially with respect to packet headers, flags and speed...Major impact to databases, DNS, provisioning and other systems. Large organizations will feel a major impact in tool-rewriting as well.”

## Concerns: “Perfect Storm”

---


- Looming IPv4 address exhaustion and the preparedness for migration to IPv6, DNSSEC and to 4-byte ASNs are contributing to a “perfect storm” scenario for Internet architecture and operations professionals
- Any one of these changes would constitute a significant architectural and operational challenge for network operators;
- Considered together, they represent the greatest and potentially most disruptive set of circumstances in the history of the Internet



“4-byte ASN represents a major concern.”

## Sample of Concluding Comments

---

- “Increasingly about money.”
  - “Attackers getting smarter, customer base clue decreasing.”
  - “More compromised customer hosts equates to more outbound DDoS.”
  - “Increased demands from banks/financial industry.”
  - “Fewer truly clueful security resources allowed and/or willing to participate in [inter-organizational] security groups, which means many security groups are filled with clueless management types.”
  - “The bad guys are beating us, badly.”
- 

# Questions

---



Full Report: [http://www.arbornetworks.com/dmdocuments/ISR2009\\_EN.pdf](http://www.arbornetworks.com/dmdocuments/ISR2009_EN.pdf)