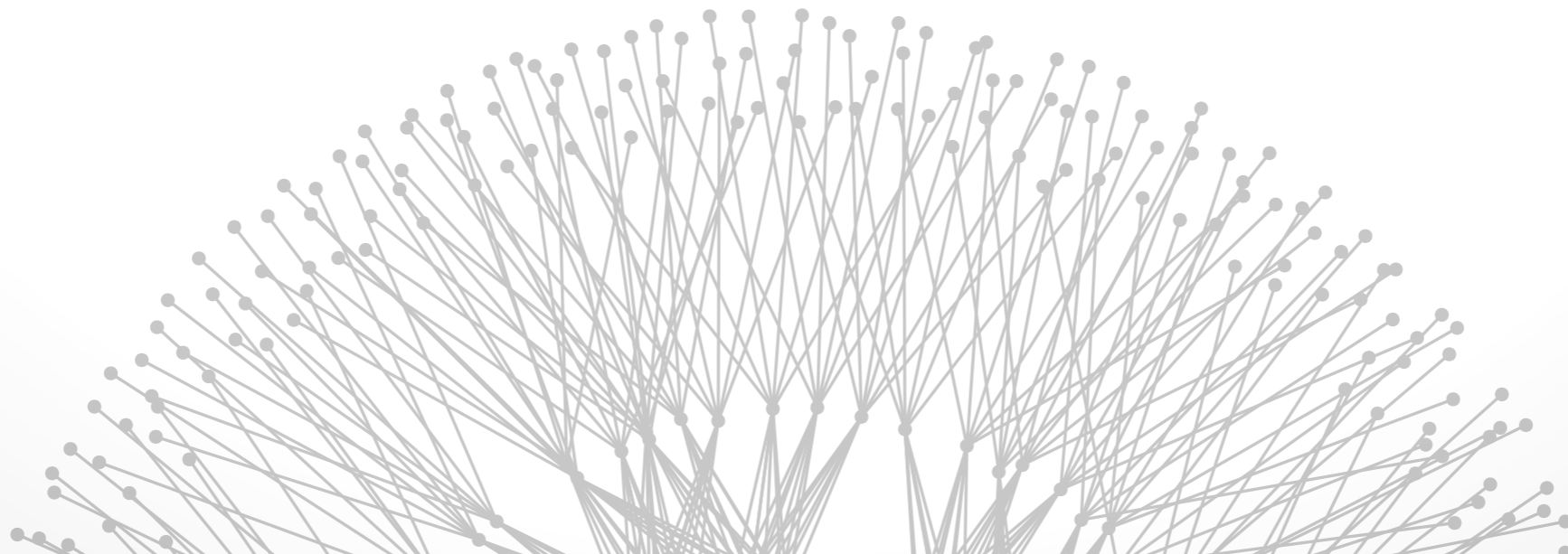


Denial of Service

Brighten Godfrey
CS 538 October 6 2011



DoS in the real world



Source: Arbor Networks

Disclaimers:

- Survey of I I I network operators, not direct measurement
- Arbor sells network security solutions :-)

DDoS is frequent and can be big



Average Number of DDoS Attacks per Month

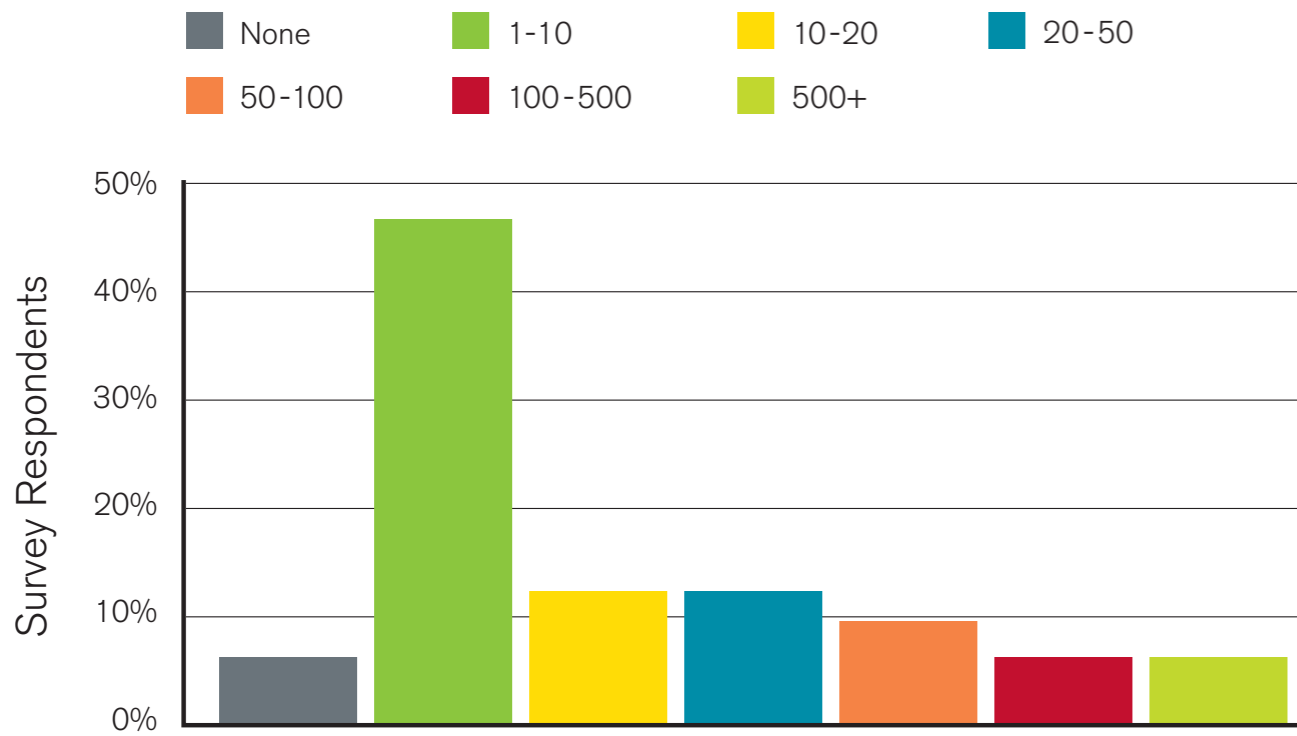


Figure 15
Source: Arbor Networks, Inc.

Largest Single DDoS Attack Observed per Survey Year in Gbps

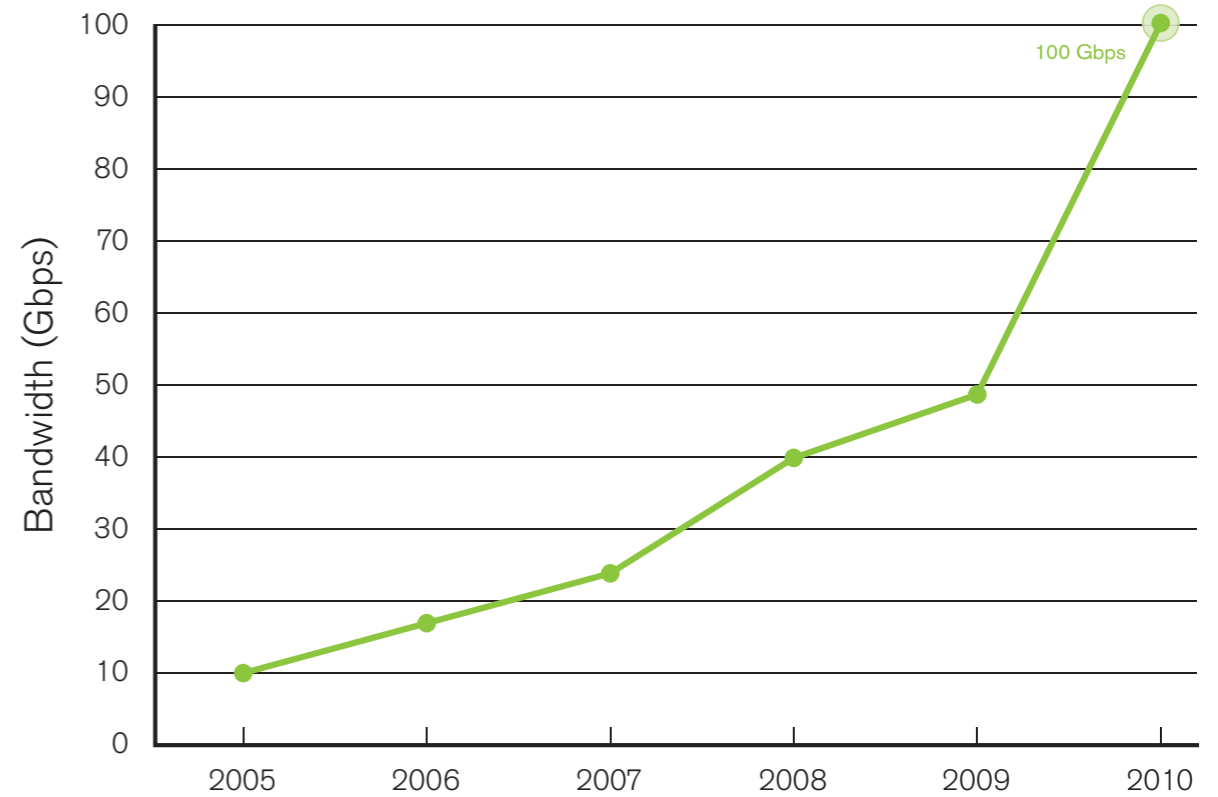


Figure 1
Source: Arbor Networks, Inc.

Types of attacks



Largest Observed Attack Vectors

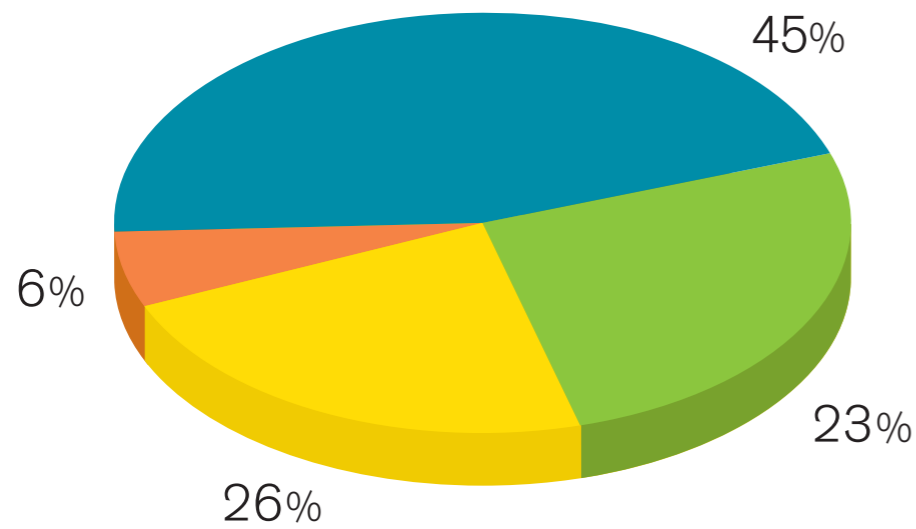


Figure 6: Largest Observed Attack Vectors

Source: Arbor Networks, Inc.

[2009 data]

- Flood-Based (e.g., UDP, ICMP)
- Protocol-Based (e.g., RST, SYN, Frag)
- Application-Based (e.g., URL, GET, DNS, SQL)
- Other

Layer 7 DDoS Attacks

- HTTP
- DNS
- SMTP
- SIP/VoIP
- HTTPS
- Other

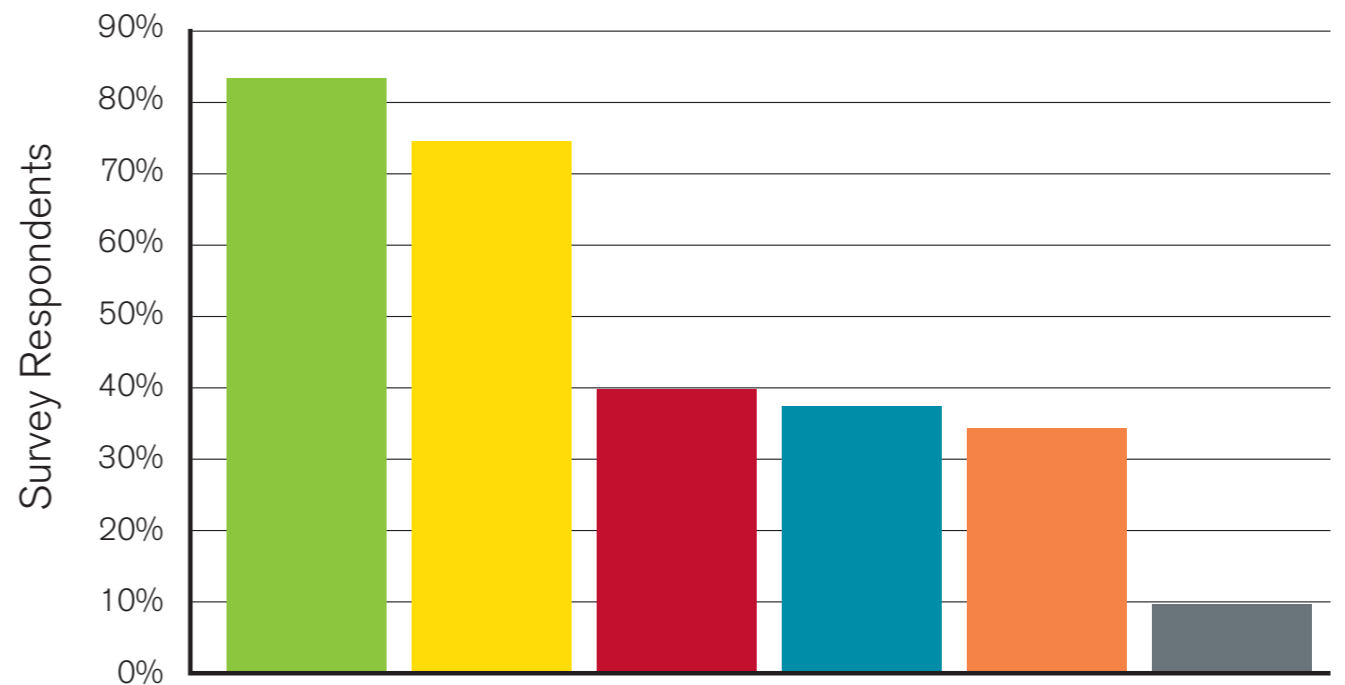


Figure 8

Source: Arbor Networks, Inc.

DDoS defense



DDoS Mitigation Tools Used



“destination-based remotely triggered blackholing”

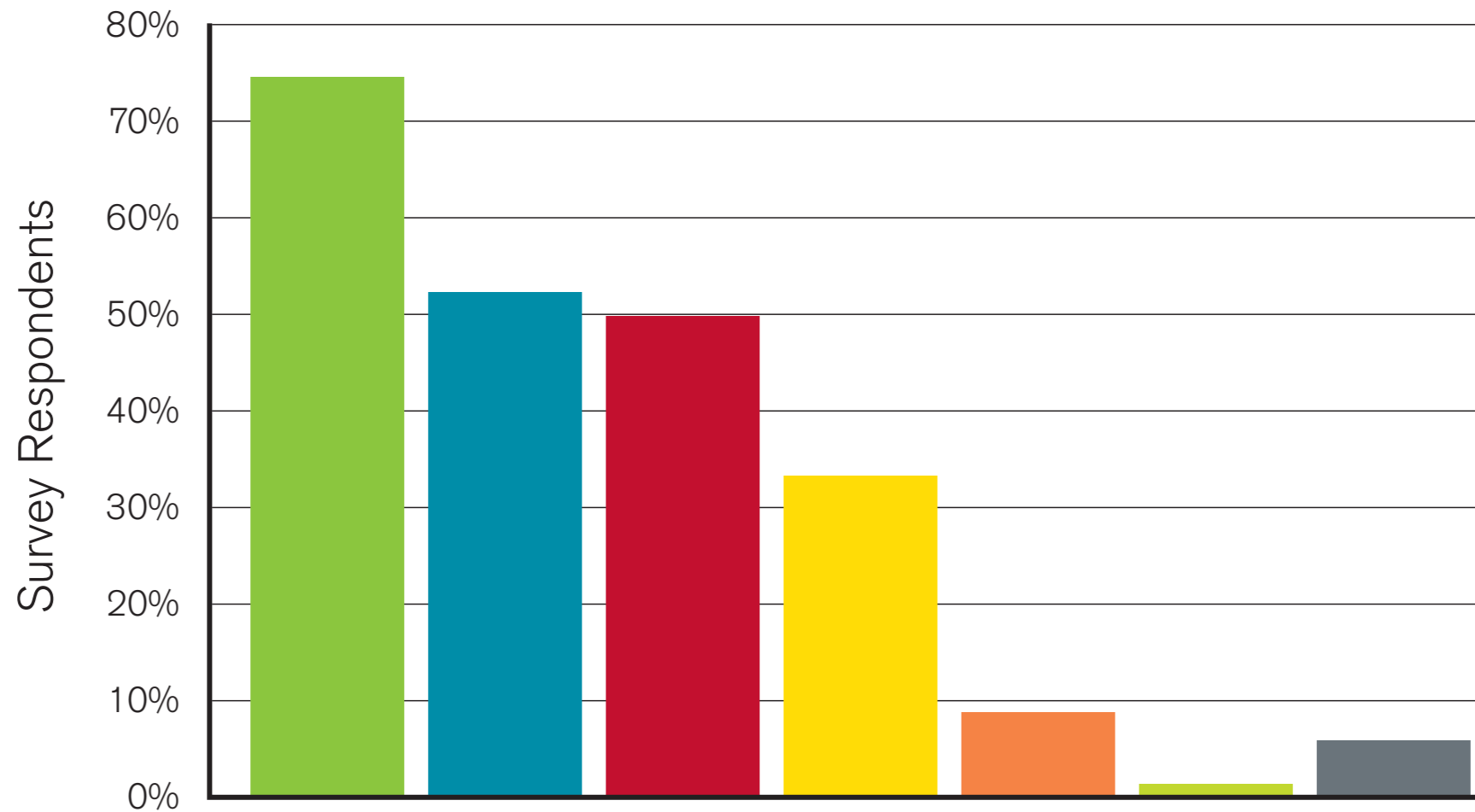


Figure 21

Source: Arbor Networks, Inc.



Most Significant Operational Threats

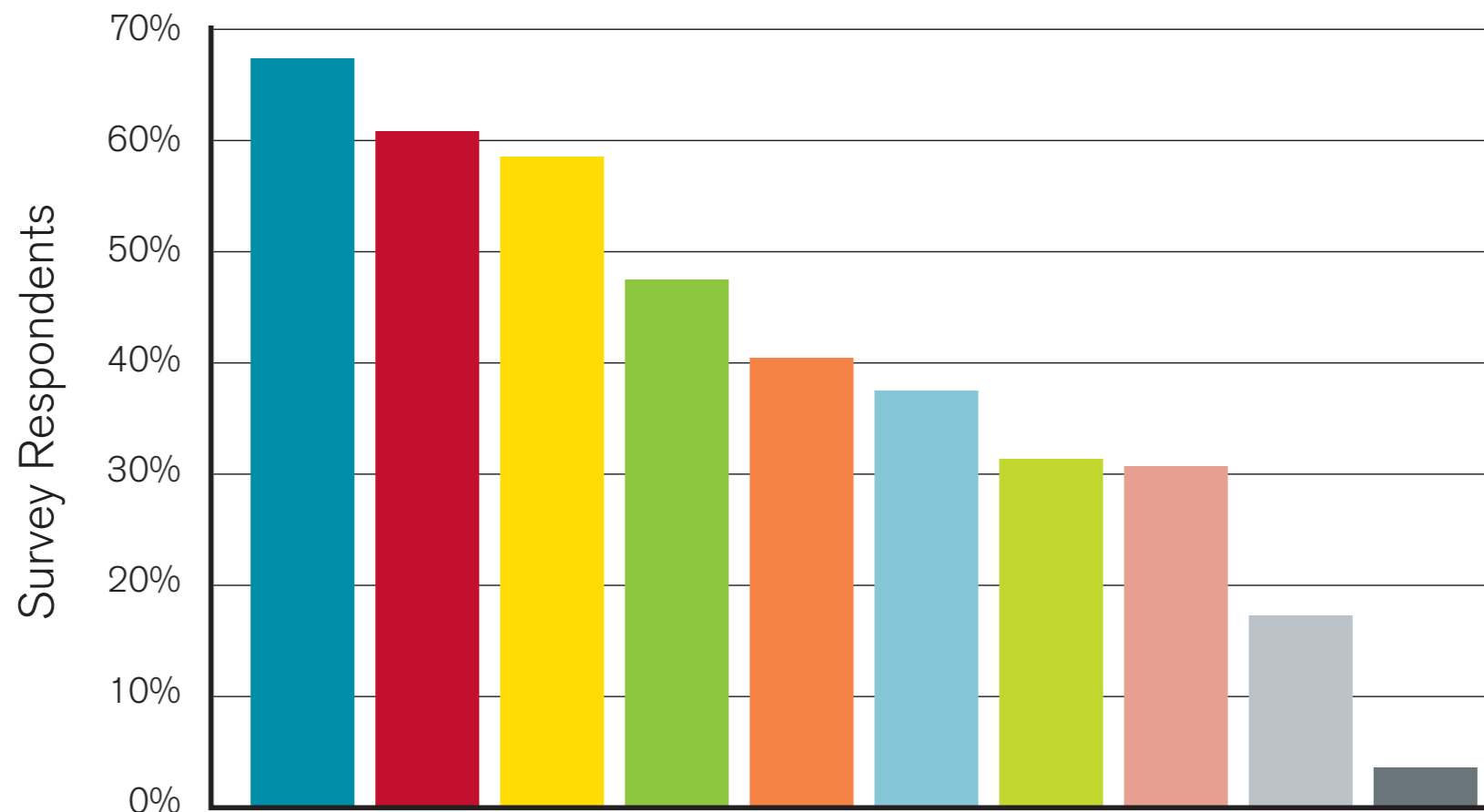
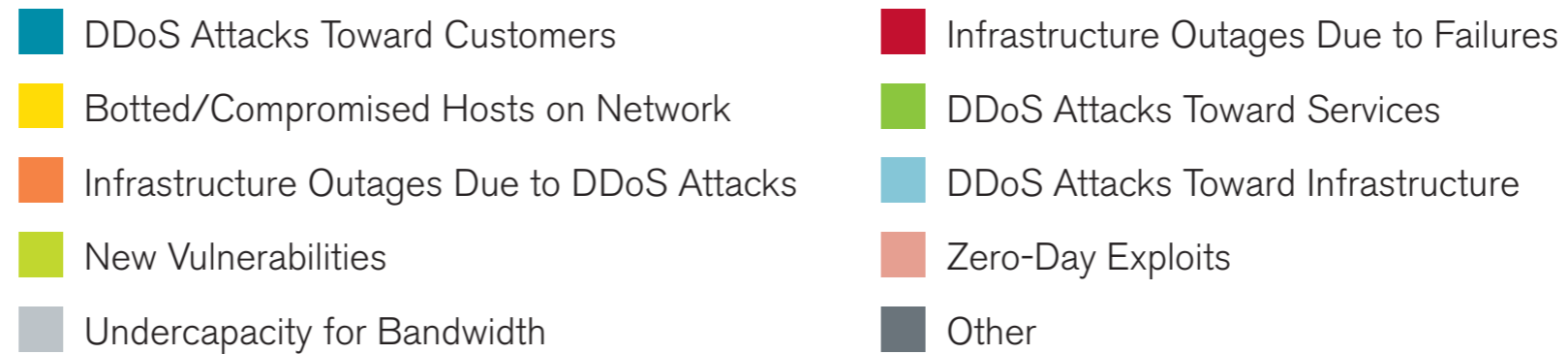


Figure 7

Source: Arbor Networks, Inc.