Update on Carrier Infrastructure Security Attacks

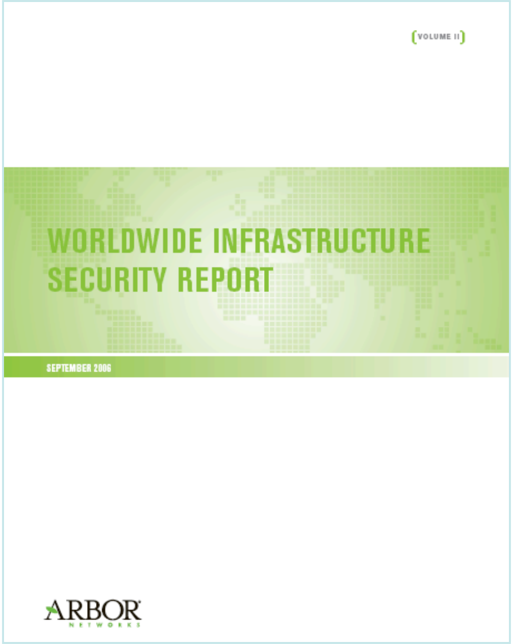
Jose Nazario, Ph.D.
jose@arbor.net

Agenda

- **Highlights of Worldwide Infrastructure Security Report**
  - Overview of Report
  - Key Findings
  - Conclusions

4th Annual Report: 2008

- **Demographics:**
  - 66 self-classified IP network operators from Americas, Europe and Asia
  - Tier 1&2 to small ISPs, large to small content, hosting, government, wireless and voice ISPs, regional & IXP network providers
  - All participants are directly involved in network security operations
- **Survey Focus:** Daily operational network security issues in commercial networks



(VOLUME II)

WORLDWIDE INFRASTRUCTURE SECURITY REPORT

SEPTEMBER 2006

ARBOR NETWORKS

- Objective:
  - Enable informed decisions about the use of network security technology for protection of mission-critical infrastructures
  - Be a general resource for trends and employment of various infrastructure security techniques

Report Highlights

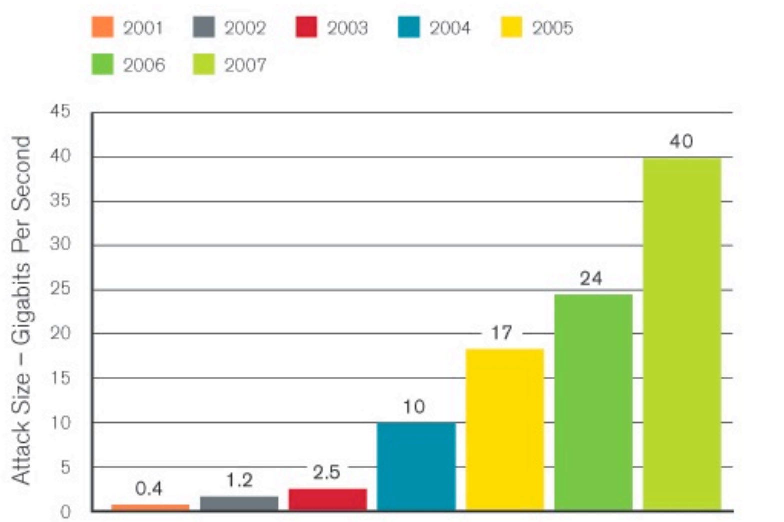
Key Findings

- Attacks are on the rise and more sophisticated – **More lower-rate highly sophisticated attacks cause more services disruption and are increasingly difficult to mitigate**
- Brute Force Attacks are growing exponentially – **A 67% increase in attack scale over the last year; 2.5x the size of the largest attack reported last year and 100-fold increase versus 2001**
- Botnets are still a concern – **26% continue to believe bots are *the* vehicle for delivering the largest problems to network operations and security engineers.**
- Operational resources are strained **– A significant increase in managed DDoS detection and mitigation services**
- Emerging threats: VoIP and IPv6 – **The scale and frequency of security threats for IPv6 will increase as it becomes more widely deployed while VoIP continues to pose a threat, though ISPs are underprepared to address it.**

Brute Force Attacks Increase

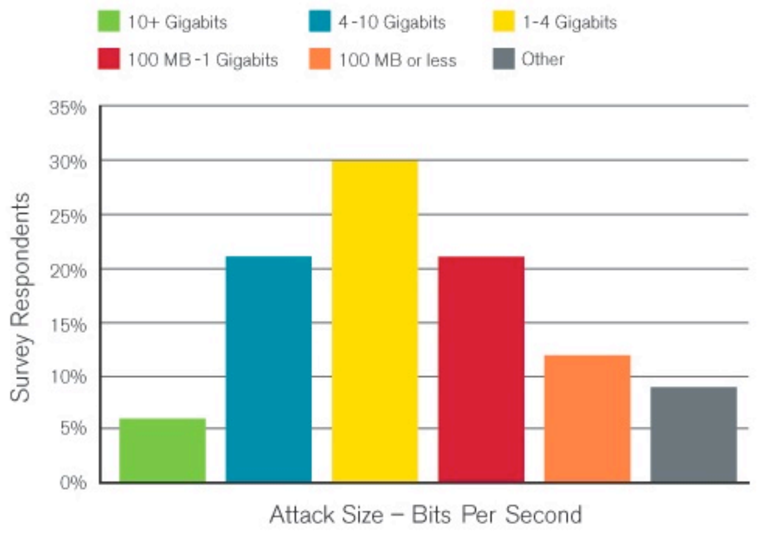
- 57% of ISPs reported attacks larger than 1 Gbps
- Largest DDoS attacks have grown 100-fold since 2001 to break the 40 gigabits-per-second barrier this year

Largest Attack Size — 40 Gigabits Per Second



Source: Arbor Networks, Inc.

Largest Attacks Observed – Past 12 Months

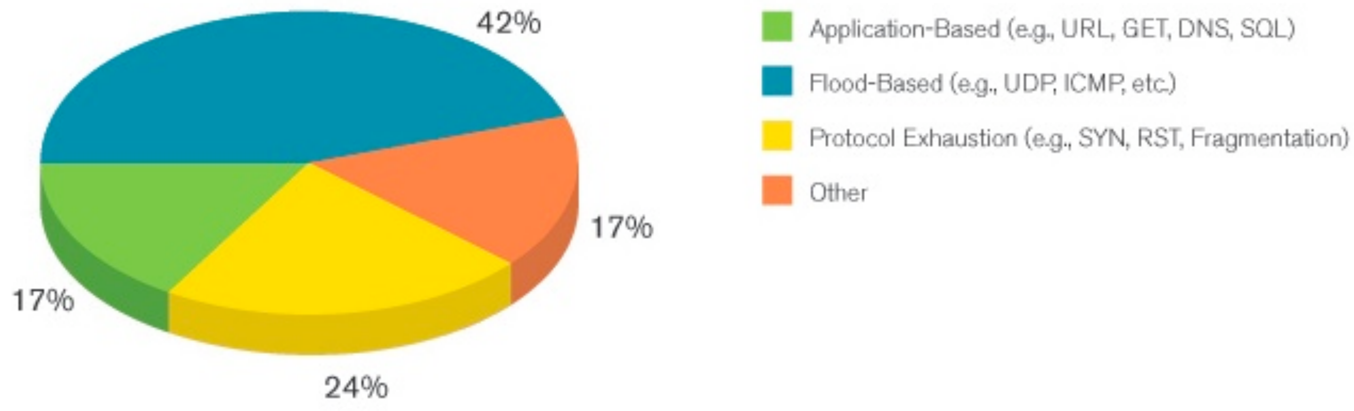


Source: Arbor Networks, Inc.

- Growth in attack size continues to significantly outpace the corresponding increase in underlying transmission speed and ISP infrastructure investment

Attacks Grow More Sophisticated

- 17% of respondents observed increasingly sophisticated attacks on network services or attacks impacting adjacent network services
- Several ISPs and content folk reported prolonged outages of prominent Internet services during the last year due to application-level attacks
- Detection and mitigation of application-layer attacks is more difficult than with flood-based attacks, necessitating surgical mitigation of attack traffic while allowing legitimate traffic to pass through

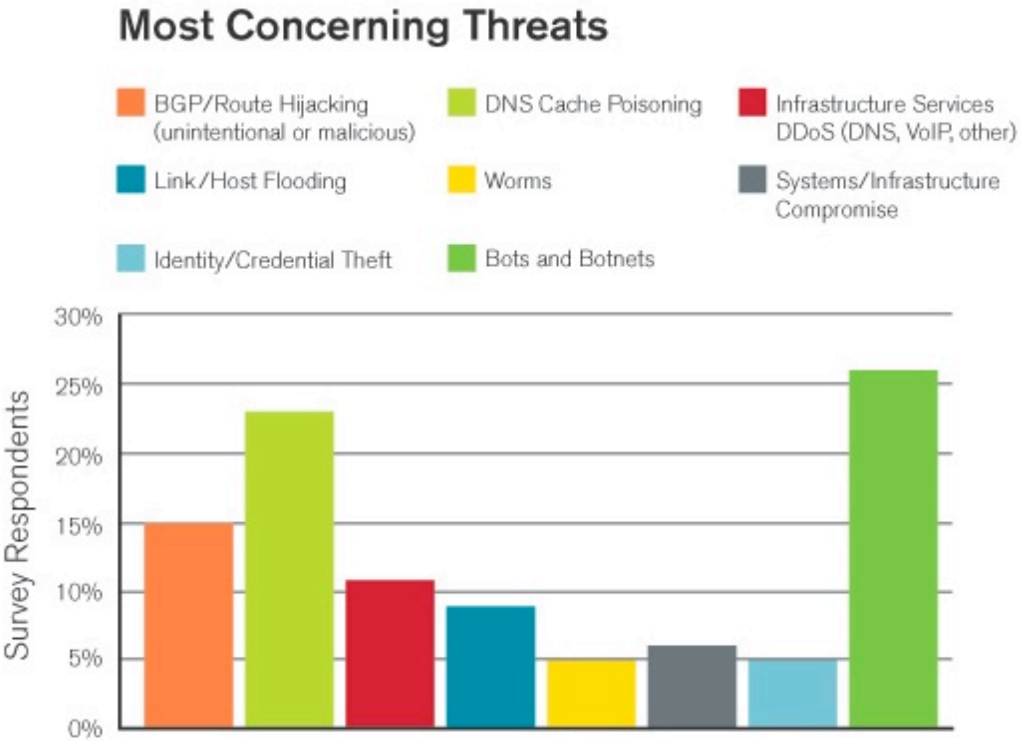


Attack Vectors

Source: Arbor Networks, Inc.

Botnets Most Concerning

- **Botnets continue to outpace other infrastructure threats**
- **Growth of the largest botnets continues to outpace containment efforts and infrastructure investment**
- **DDoS flooding of links and hosts fell from 24% last year to 11% this year, likely reflecting the increased ability of ISPs to mitigate these types of attacks**
- **Uptick in DNS concerns likely attribute to timing of Kaminsky work and survey response, BGP uptick, likely because of press w/Youtube, L-Root, etc..**



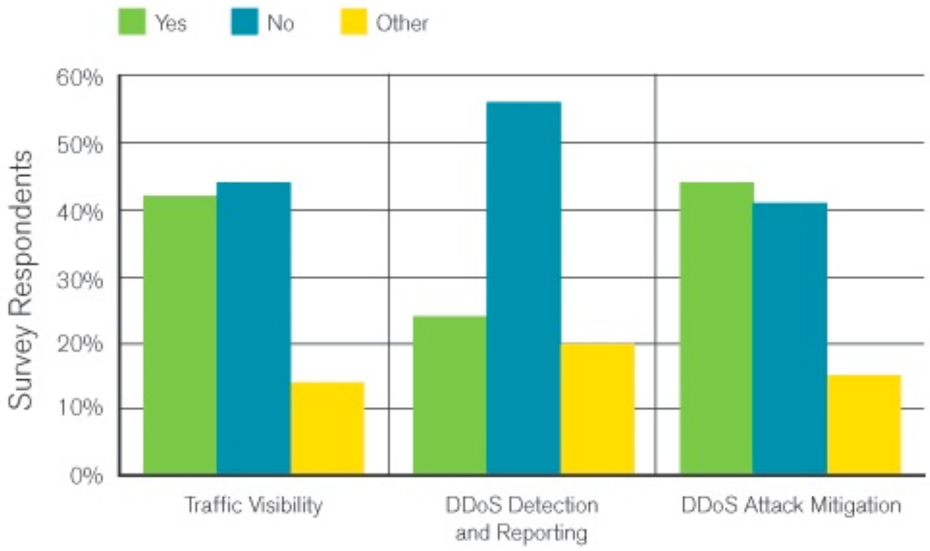
Source: Arbor Networks, Inc.

Strained Resources, More MSS

- Service providers are facing increasing cost and revenue pressure in a slowing global economy

- Organizations are turning to Managed Security Services (MSS) – network security management from service providers

Revenue-Generating Customer Service Offerings



Source: Arbor Networks, Inc.

- ISPs are increasingly deploying more complex distributed VoIP, video and IP services

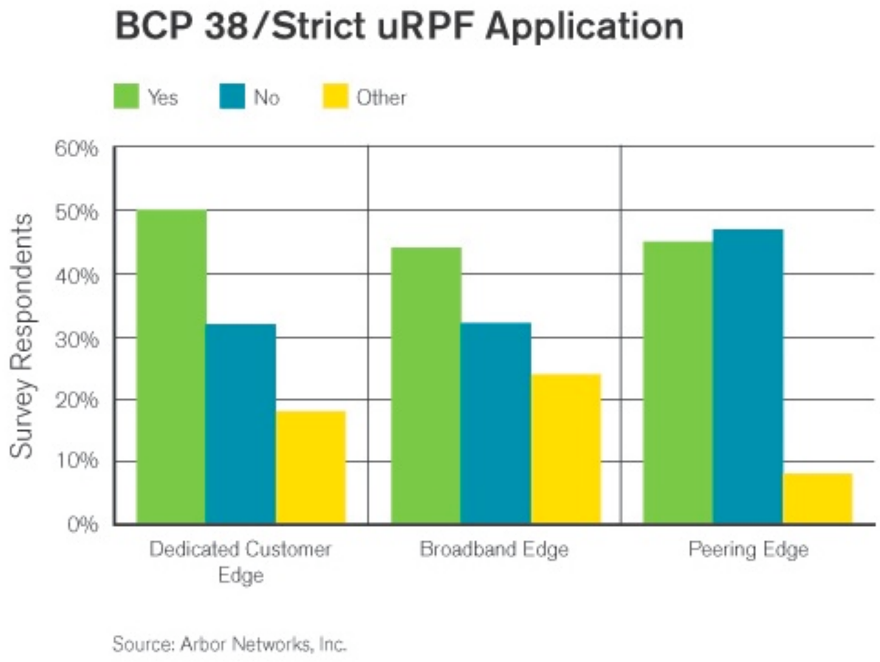
- However, surveyed ISP security engineers also say these new services are often poorly prepared to deal with the new Internet security threats

Emerging Threats

- Top emerging threat vector:
  - DNS cache poisoning
  - BGP Route hijacking
  - both saw much PR in 2008
- Additional emerging threats: IPv6 and VoIP
  - ISPs are deploying more complex distributed VoIP, video and IP services – represents a growing threat to the infrastructure
  - 55% of ISPs identified scale and frequency of threats for IPv6 as an increasing threat vector
  - Overall, providers are underprepared to protect their VoIP infrastructure from attack
    - Only 21% of respondents have tools in place to detect threats against VoIP infrastructure or services

Anti-Spoofing Techniques

- In general, application of anti-spoofing worse than illustrated here, as respondent pool assumed slightly more clueful than larger operator set

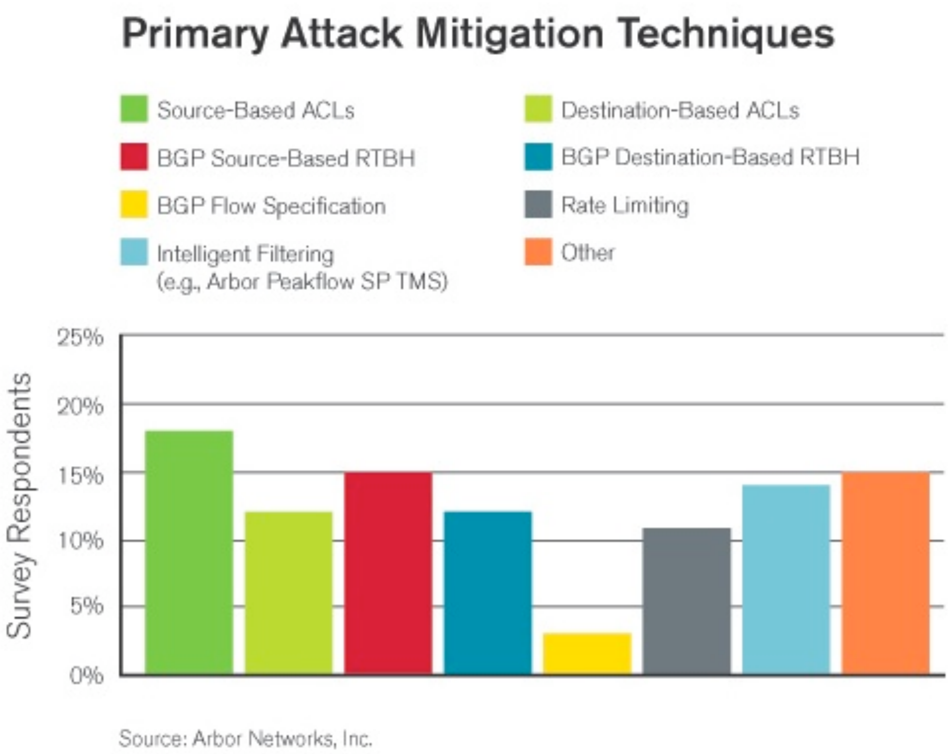


Source: Arbor Networks, Inc.

- Application of anti-spoofing techniques improves slightly, still dismal
- Loose mode uRPF creates false sense of value, as legitimate source IPs can still be spoofed
- Reflection attacks, cache poisoning, etc.., all employ source address spoofing

Attack Mitigation Techniques Improving .. Slightly..

- Traditional techniques, destination-based ACLs, BGP RTBH effectively completed attack
- Continued uptick in more intelligent filtering, required for application level attacks
- More fine-grained and source-based, and surgical mitigation devices allow for attack mitigation and forensics collections will preserving legitimate traffic flows



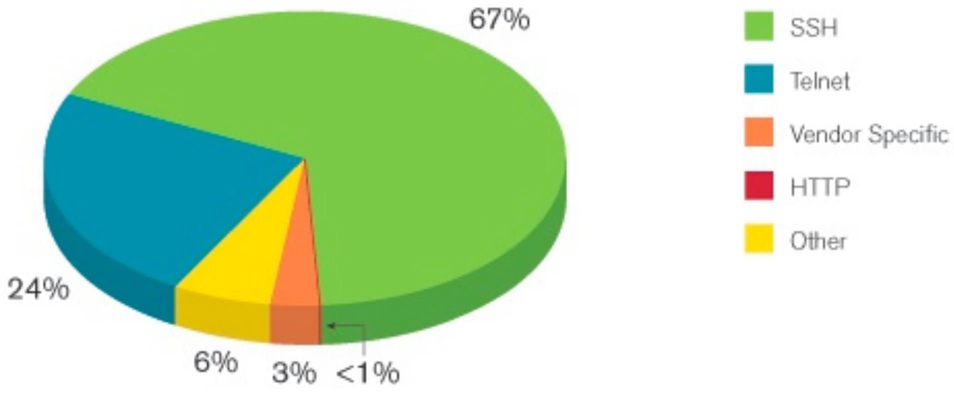
Primary Attack Mitigation Techniques

Source: Arbor Networks, Inc.

Infrastructure Access

- SSH most common for CLI/shell access
- 24% still use telnet - beware those sniffers anywhere in transaction path!

Mechanisms Used to Access and Configure Network Devices

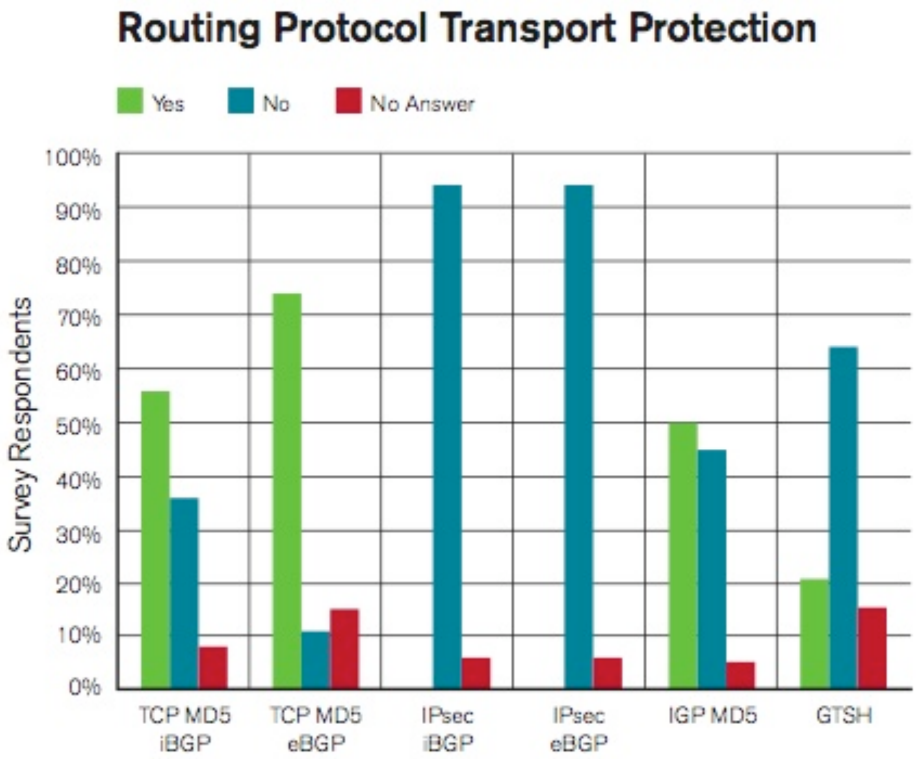


Source: Arbor Networks, Inc.

- 45% of respondents indicated that they still use SNMPv1, while only 17% have migrated to SNMPv3, which is far more secure
- Some 20% of respondents indicated that they do enable SNMP write access on network devices - which means some use SNMPv1 with write access - ill-advised!

Routing Transport Security

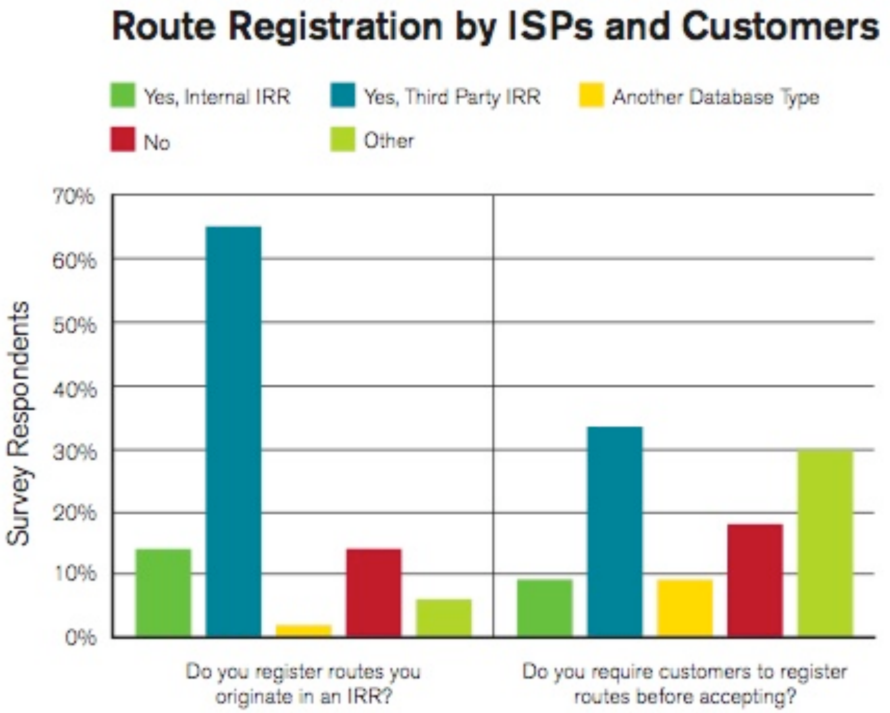
- TCP MD5 signature option most common BGP transport protection, not applied ubiquitously
- Application varies internally, between customers and peers
- Infrastructure ACLs (iACLs) and Generalized TTL Security Hack (GTSH) best way to protect BGP transport



Route Filtering Application

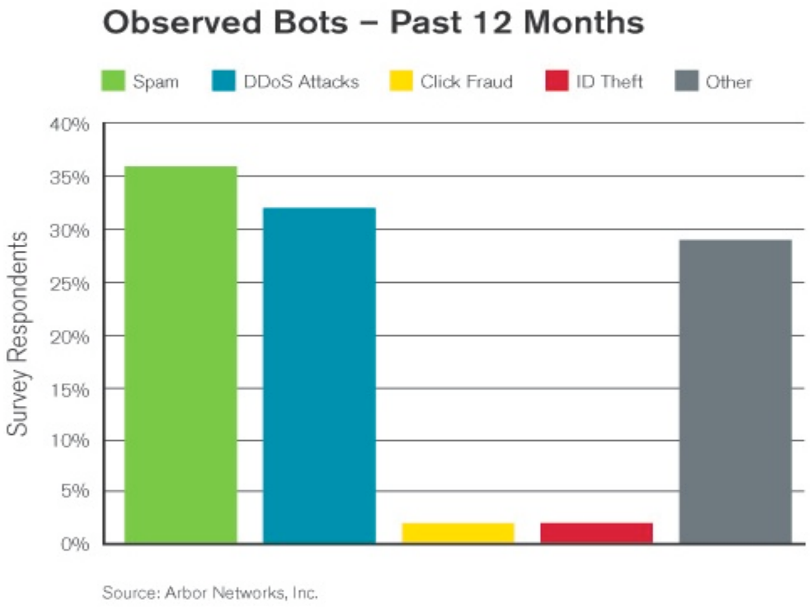
- Very little explicit prefix filtering today
- Most filtering for self-originated routes, then customer-originated routes
- Virtually nil explicit prefix filtering for ISP peers

- Lacking Resource PKI (RPKI) and subsequent employment by network operators routing security will only continue to deteriorate
- Operators should be VERY concerned about this!



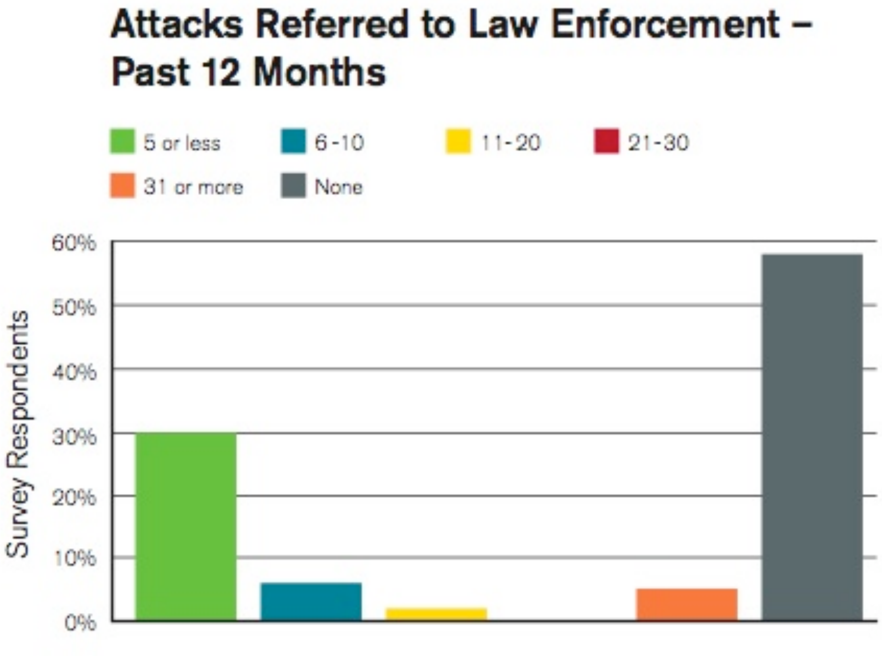
Botnet Employment

- Primary reported botnet employment: Spam and DDoS lead the pack, as usual
- Spam was also reported as most resource intensive operational security related threat
- More reports of click fraud from content folk



Law Enforcement

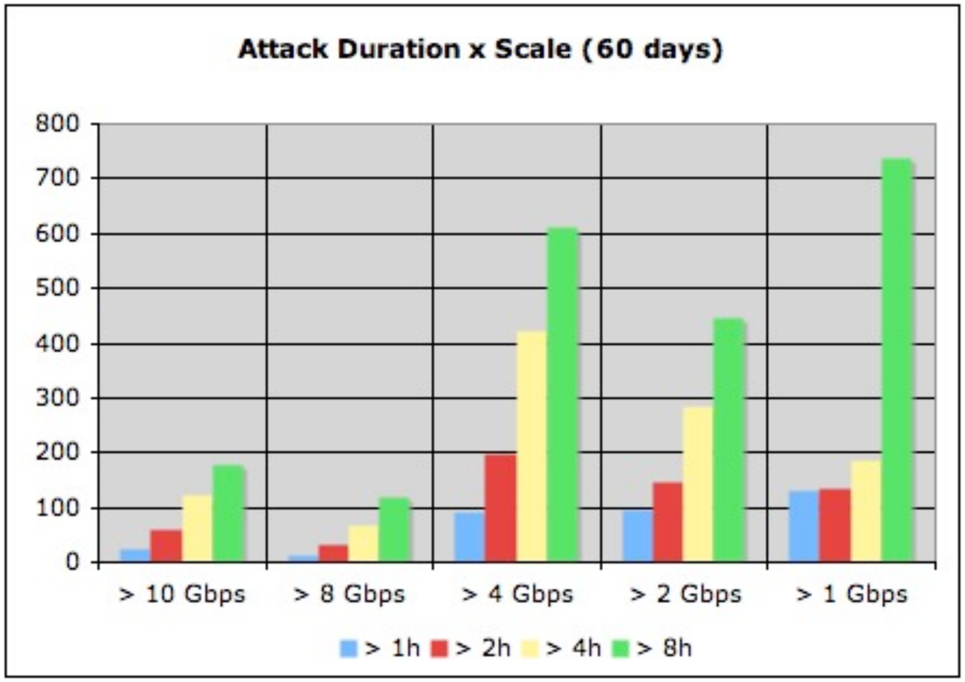
- 29% reported law enforcement's limited capabilities limits referred attacks, while 26% said they expect customers to report, and 17% indicated they believe there is little or no utility in reporting attacks to LE
- 8% increase (to 58%) in the number of respondents that said they reported no incidents to law enforcement over the past 12 months
- Much more detail on this in the report



Incident Response Teams & CERTS

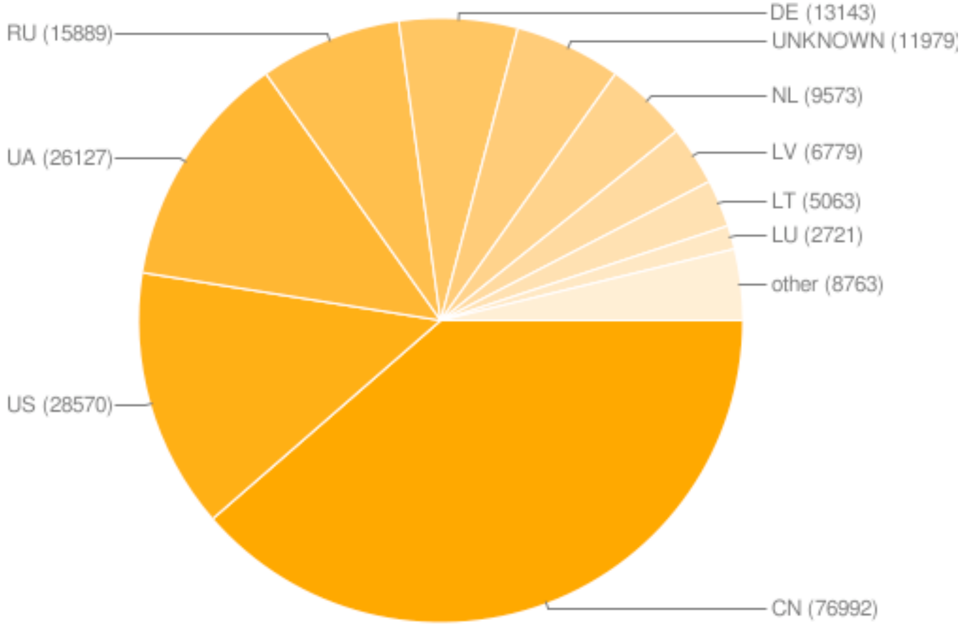
- Only 45% of respondents indicated they currently have IRT/ERT teams, and a corresponding 45% (not surprisingly) indicated they worked with other operator or national CERTs
- 77% indicated that they believe national CERTs DO have a role in operational security
- Even the smallest organizations should have IRTs and incident response plans
- Another 18% said national CERT failure stems from a lack of cooperation with network operators, while 15 percent said the failure is due to lack of regulation, policy or legislation.
- Nearly 23 percent said governments fail to enable infrastructure protection because they are slow and far too political
- 11% said they seem to be doing a decent job.

Spring 2009: Attack Durations



- Actual attack traffic
- Peak attack sizes
- Attack start and end is consistently over 8 hours

2009 Q2 Botnet C&C



Data from Bladerunner project

Active botnet tracking

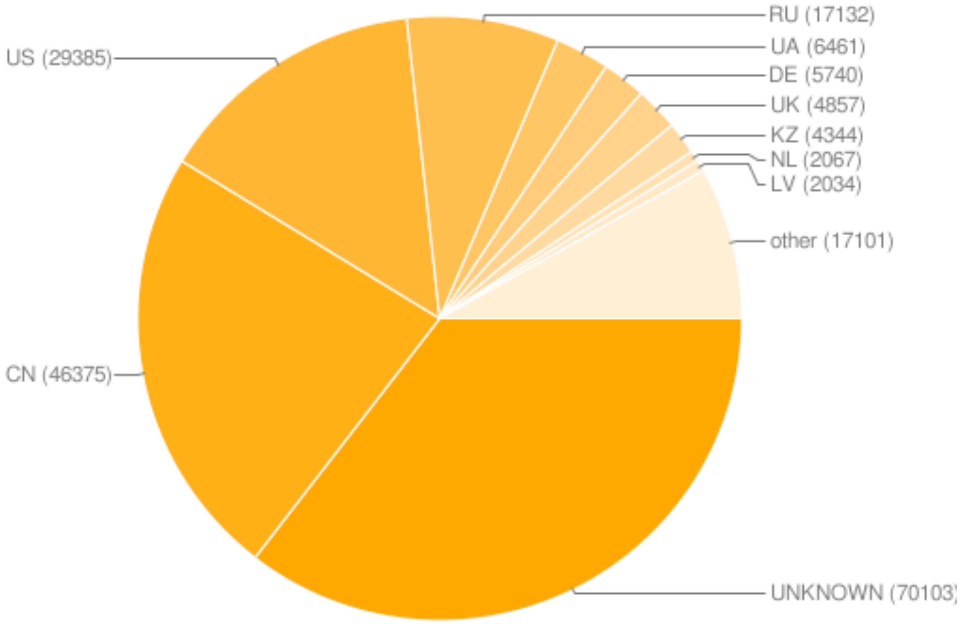
Biased by what we know

CN-CN attacks most common

- US, RU etc attacks popular, dispersed globally

2009 Q2 Botnet Victims

- Bladerunner data, active command logging
- Long term history of botnets
- Continued attacks on casinos, porn sites, etc



Pressing Attacks, Growing

- DNS servers weakest link

- DNS amplification
  - IN/SOA for . … 20x+ attacks
  - Collateral damage with amplifiers
- DNS servers floods
  - ICMP, SYN, UDP floods
- DNS server stress
  - Dictionary walks, etc

- Need to identify botnet, tools

Power of RFI Attacks

- PHP bots
- PHP attack botnets

- No tracking
- No visibility into who it is

- 1000s of new bots every day

Conclusions

- **Attack continue to grow in size, frequency and sophistication**
- **As a result, ISPs describe a double-edged struggle as they face increased cost and revenue pressure**
  - They are increasingly deploying more complex distributed VoIP, Video and IP Services to generate additional revenue streams and require higher levels of service availability and security
- **While most ISPs now have the infrastructure to detect bandwidth flood attacks, many still lack the ability to rapidly mitigate these and more sophisticated attacks**
- Much more detail is available in the report itself, and the authors most certainly welcome comments, corrections and feedback
  - http://www.arbornetworks.com/report

Things Not Covered Here

- Route security
  - BGP-S and sBGP
  - Routing registries
  - E.g. Pakistan-YouTube route hijack
- Securing DNS
  - DNSsec deployments
  - Anti-Kaminsky (70% adoption via DNS-OARC)

Thank You