SP Infrastructure Security Survey Results

FRNOG 7

Paris, France

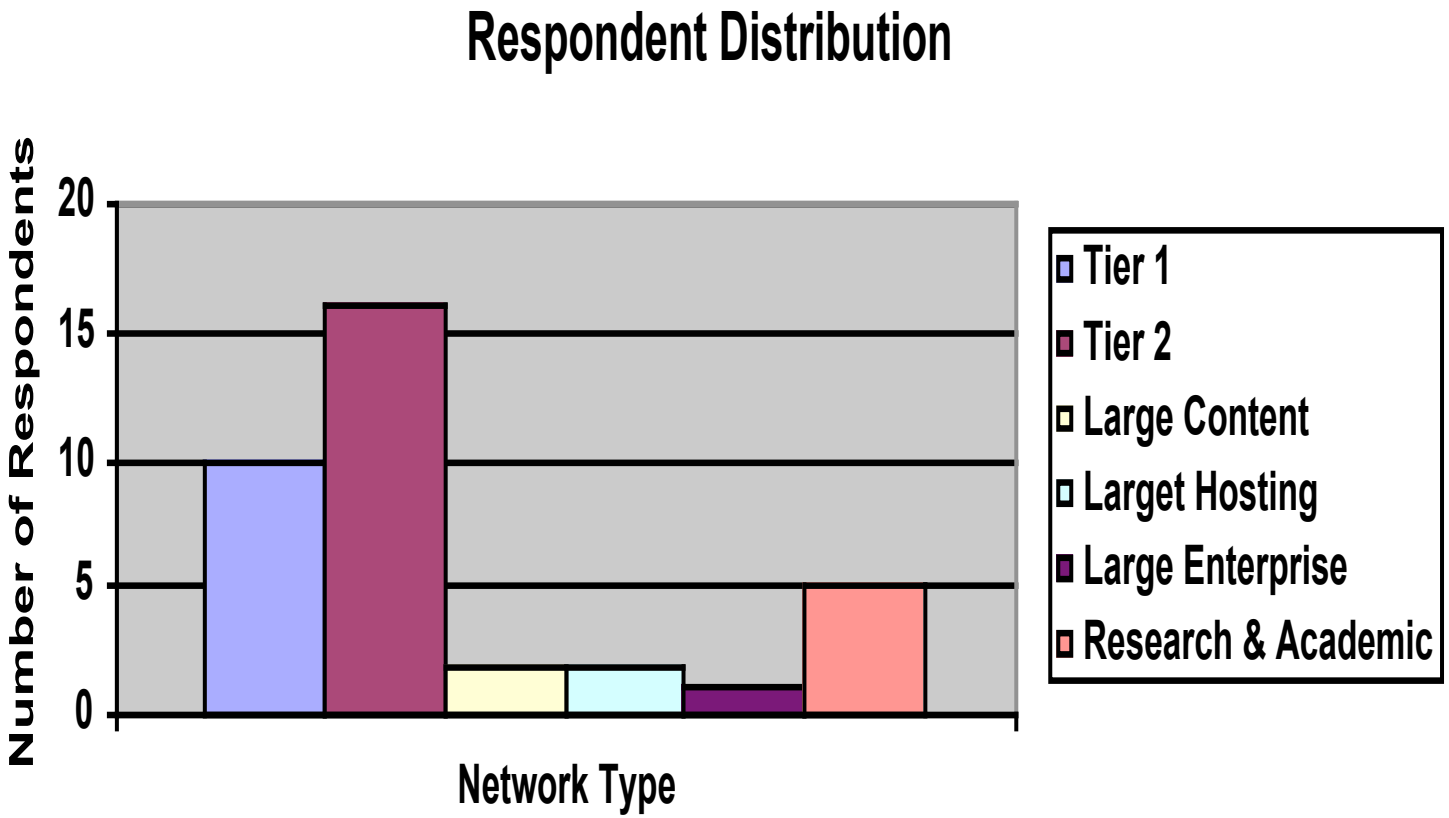
Danny McPherson danny@arbor.net

18 NOV 2005

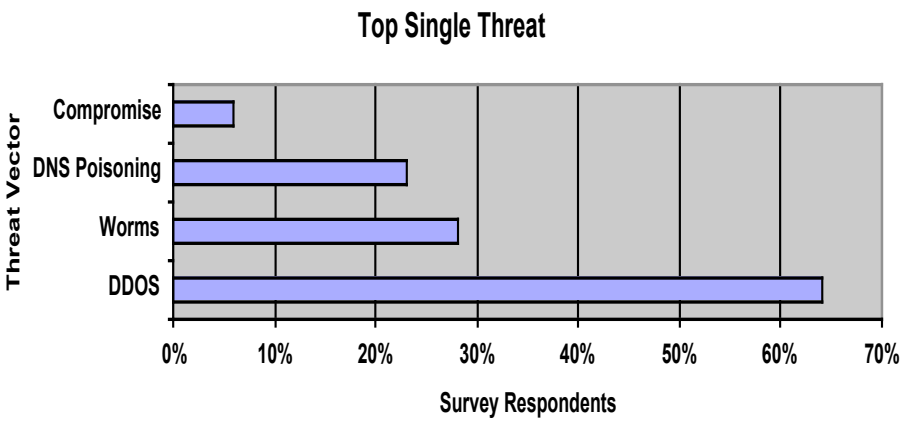
Background

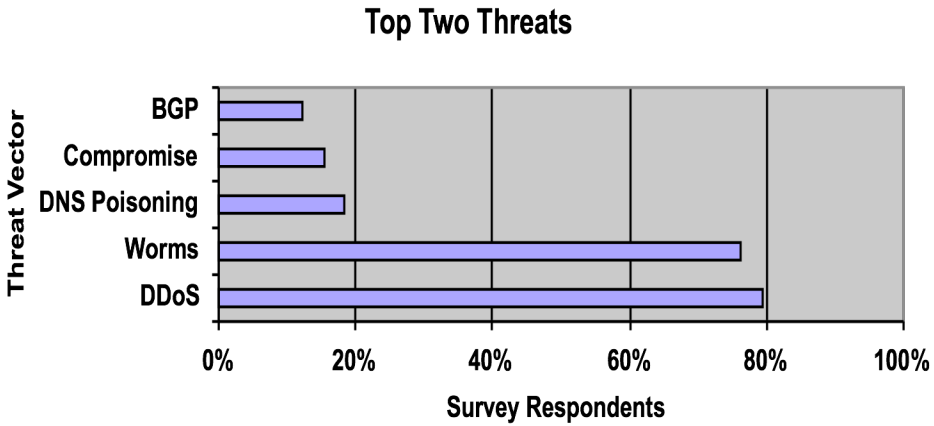
- Earlier this year a survey was conducted among network security operators
- The survey was targeted at obtaining an understanding of some of the operational security aspects occurring in large Internet networks today
- 36 network operators responded to the survey - some responses were, hrmm.. less than trivial to parse
- The survey was composed of 32 multiple choice and free response questions
- The findings of this survey are reflects in the following slides
- Some of you may have seen this data presented at NANOG 35

Survey Respondents



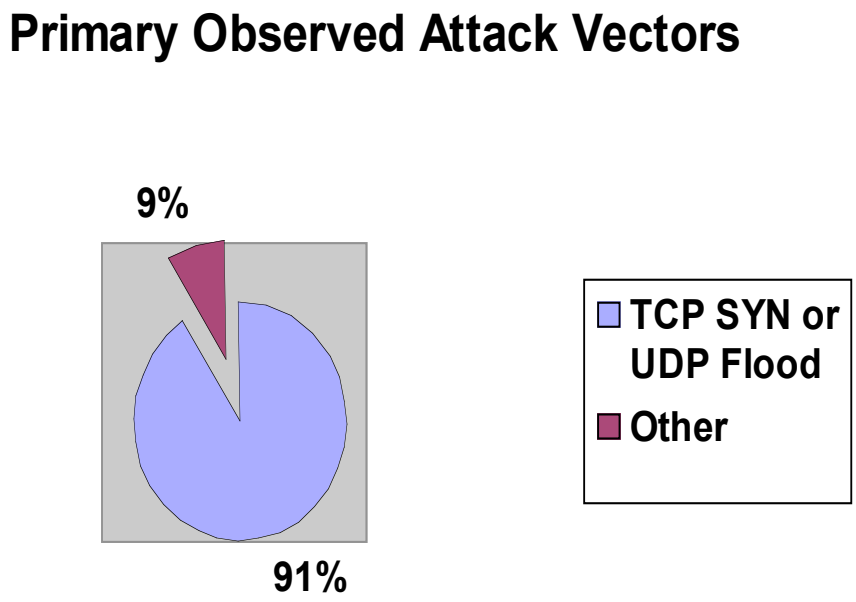
Primary Threat Concerns





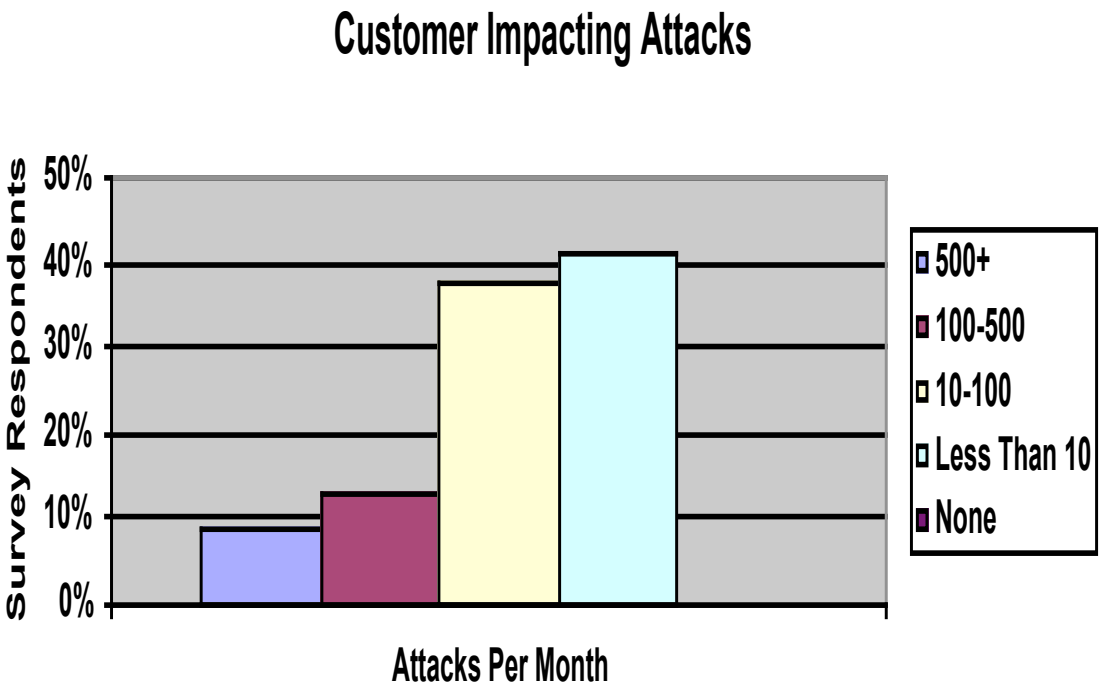
- DDOS was top concern, with worms coming in second
- Implicit DOS impacts of worm more concerning than worm payload itself
- BGP vulnerabilities weren't listed as anyone's top concern

Attack Vectors



- While TCP SYN and UDP flooding “brute-force” attacks were most commonly observed actionable attacks, more sophisticated attacks such as multi-modal and Application Layer attacks were reported as well

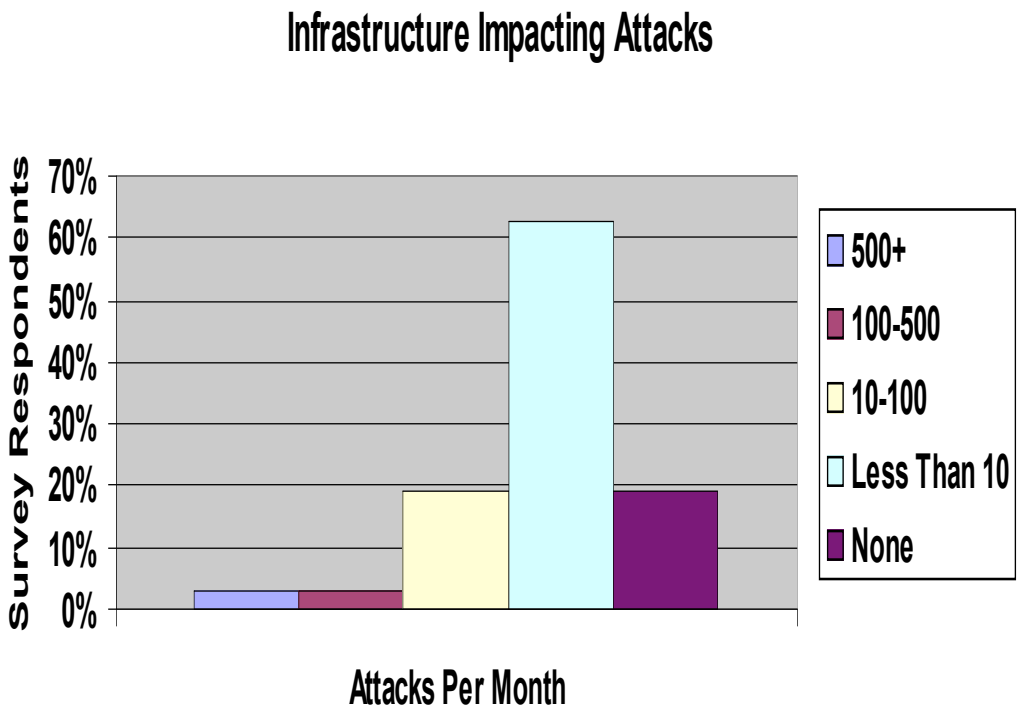
Customer Impacting Attacks



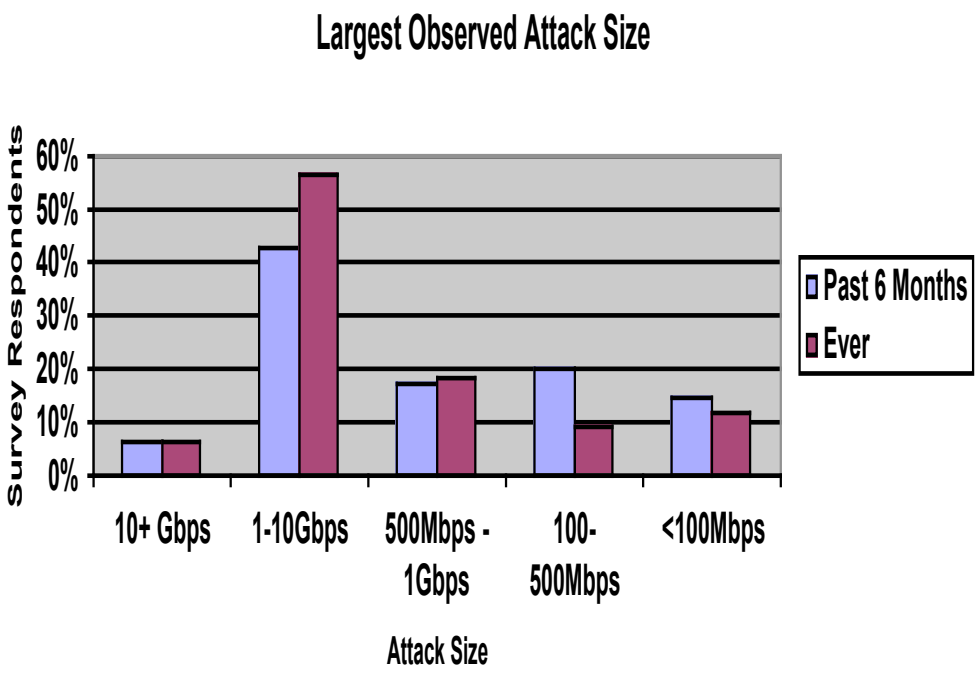
- An average of 40 actionable customer impact attacks per month were reported

Infrastructure Impacting Attacks

- Infrastructure impacting attacks were far less common, on the order of 1-2 per month on average
- These attacks were targeted directly at the infrastructure, as well as a result of collateral damage from customer attacks



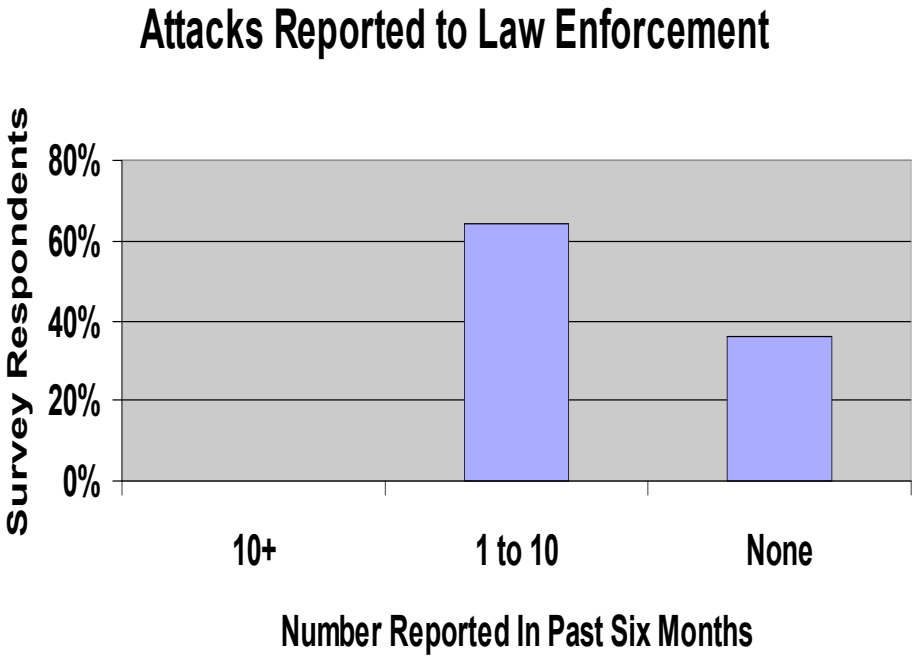
Largest Attacks Observed



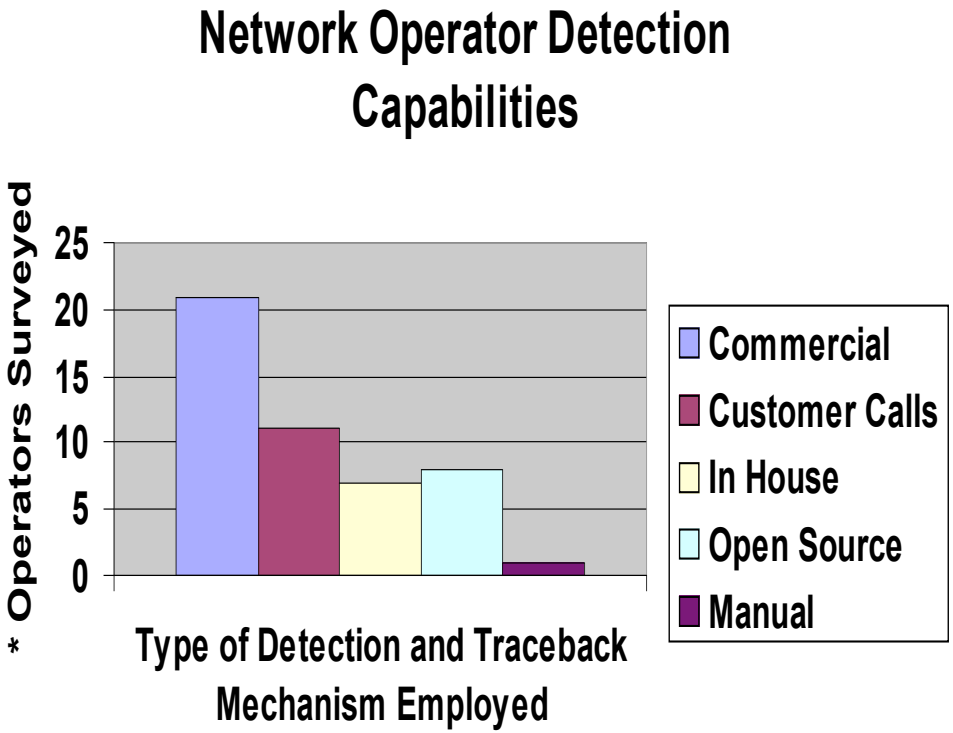
- Attacks greater than 10 Gbps sustained bandwidth were reported
- Not a large differential in largest attack ever v. largest in past six months - perhaps indicative of worsening problem

Attacks Reported to Law Enforcement

- Of **actionable** attacks, only ~1.5% are reported to law enforcement agencies
- Some of the reasoning provided:
  - Jurisdictional issue
  - Online gambling techniquely illegal is US
  - IRC users unloved
  - Customer profiles - they don't want attacks recorded
  - Lack of evidence and forensics data
  - Large amount of uncertainty from legal department

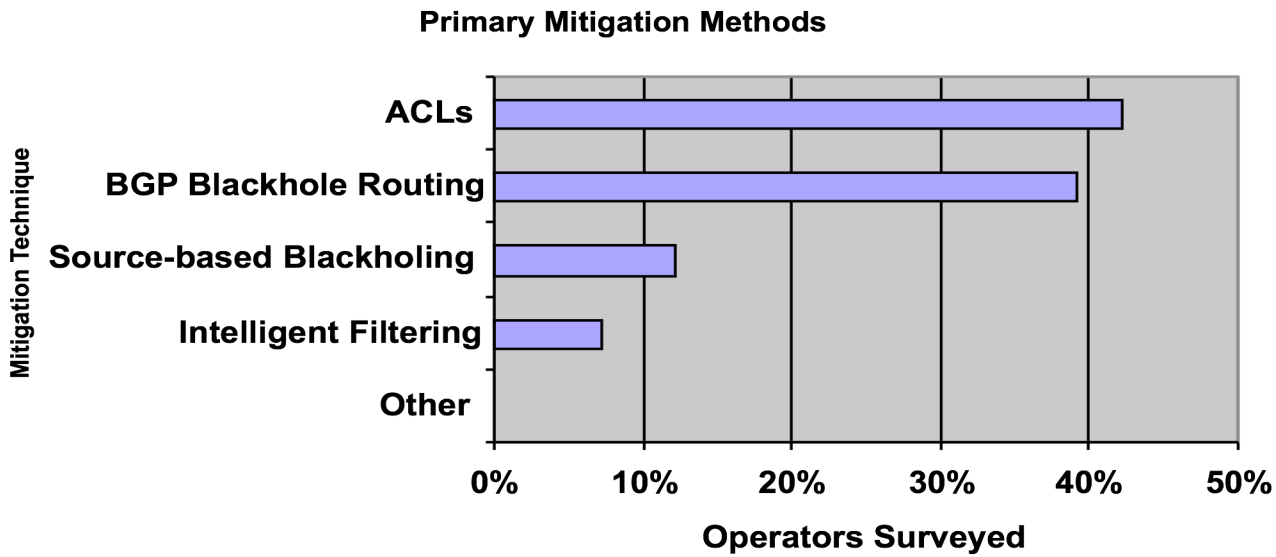


Attack Detection Capabilities



- Most operators had some commercial tools in place, though not covering the entire network perimeter
- Most providers employed multiple mechanisms for attack detection
- ISPs in wholesale/transit mostly rely on NOC trouble tickets (i.e., customer calls)

Mitigation Techniques



- The primary mitigation techniques employed by operators involve effectively completing the attack!

Botnet Observations

- No noticeable trends in sizing of botnets from respondents - although attacks are appearing to be better organized
- Few reported any tools used to track botnets
- One provider indicated that the botnets appeared smaller, but much better organized. This provider described large pools of “reinforcements” that joined the attack as the provider initiated different mitigation efforts. Another provider described armies comprised of “divisions” of smaller groups, noting: “the little bastards appear to be learning actual military tactics.”

DDoS Overview: What is Under Attack?

- Most frequently attacked sites include:
  - IRC servers
  - Gambling, especially offshore
  - Porn sites

- Additional survey reports included:
  - Residential users
  - Web hosting
  - The Chinese
  - RIAA related sites

Security Teams

- Quite a variation in size and reporting structure for security teams across respondent organizations
- Some tier-1s had dedicated infrastructure security teams of as many as 9 full-time employees, others had only 2-4, many of whom were also responsible for backbone engineering functions
- Residential broadband and dial-up providers seemed to have the largest security-related organizations
- Across all respondents, approximately 50% of the security teams were part of network engineering, 25% were part of operations, and 25% were an independent entity
- Some respondents privately complained that the design/architecture teams have no responsibility for the edge and beyond

Social Engineering

- Large European provider had internal tiger team successfully phish security/authentication information from NOC
- Social Engineering will always be a factor - be sure to factor in processes and policies, audits, etc..

Conclusions….

- DDOS is still the primary concern for network security operations
- Brute-force attacks most popular and clearly effective
- Detection and mitigation mechanisms need to improve and be deployed ubiquitously
- Until miscreants are prosecuted it's unlikely things will get better
- Tools and staffing are a major factor in operator response capabilities

About the Survey

- Plan to conduct bi-annually
- Thanks to all those that responded or reviewed the results
- Hope to get more details and pose less ambiguous questions in future revisions
- Full survey report can be found here:
  - http://NEED-TO-POST

Thanks!