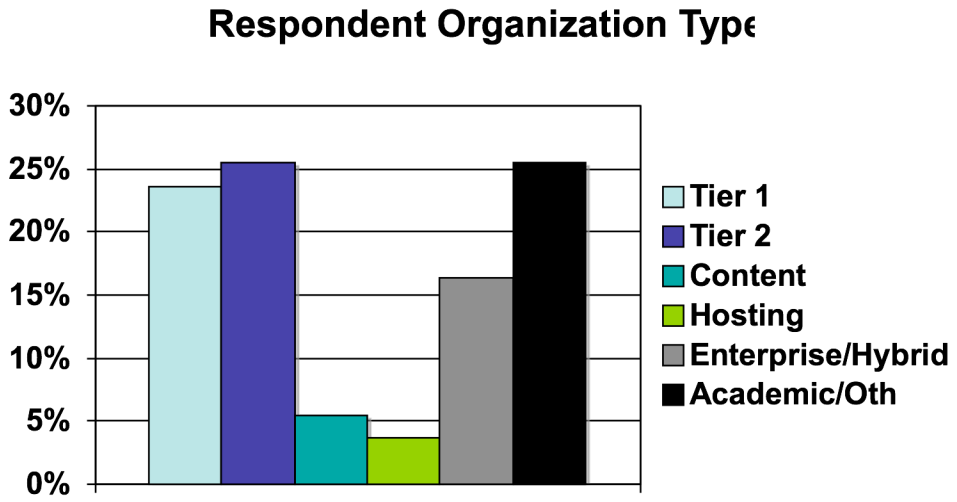
Infrastructure Security Survey

RIPE 52 - Istanbul, Turkey

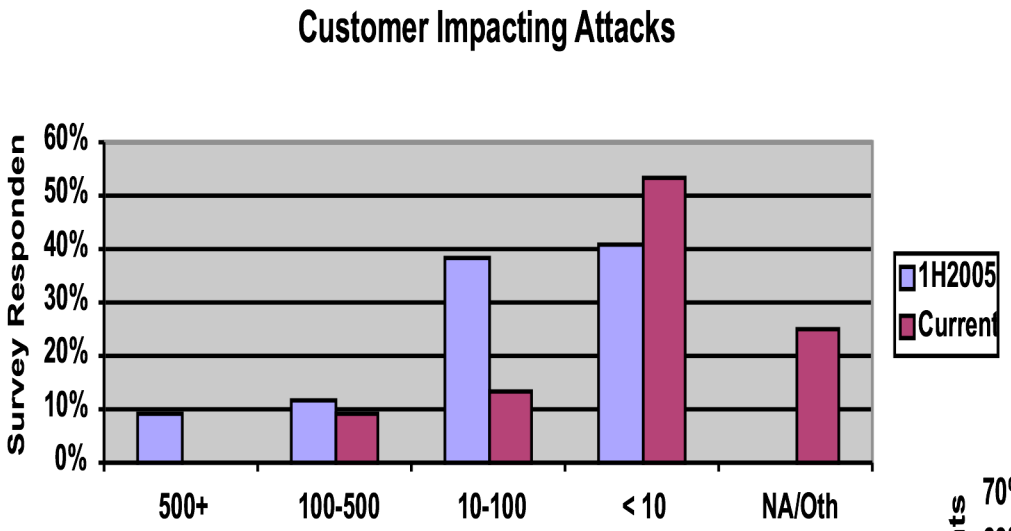
What's in a DOS Attack?

Overview

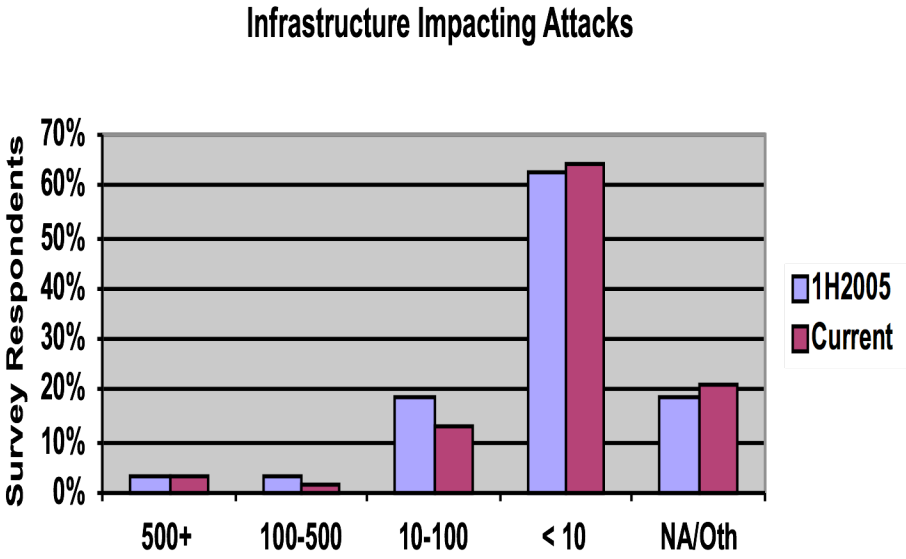
- Bi-annual survey, second edition representing 2H2005
- 55 respondents from network security operators - 65% increase from previous edition
- Respondents distributed across Tier-1, Tier-2, Large Content, Hosting, Academic & Enterprise networks - self categorized



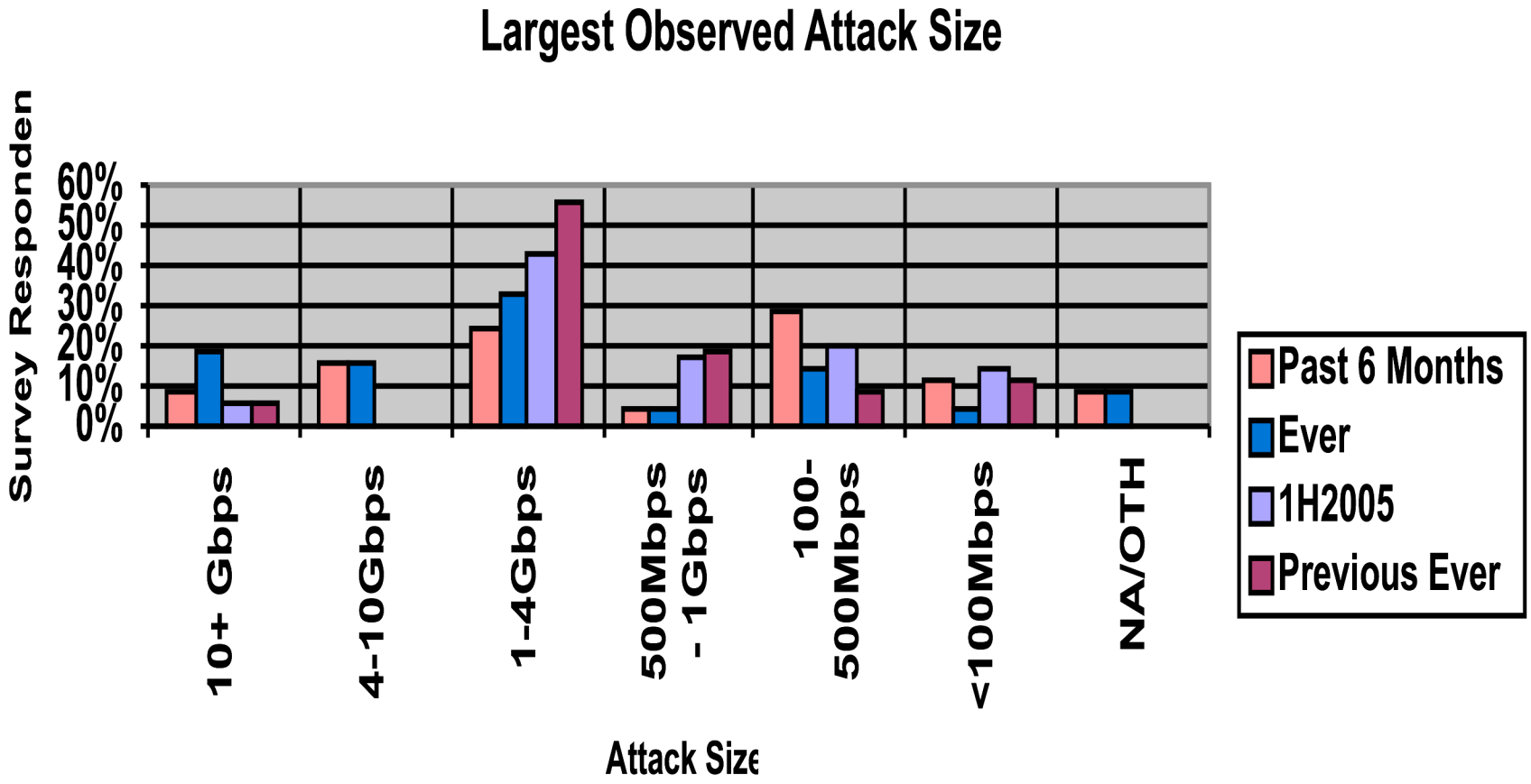
Impacting Attacks



Actionable attacks only, infrastructure attacks may have been resultant of collateral damage



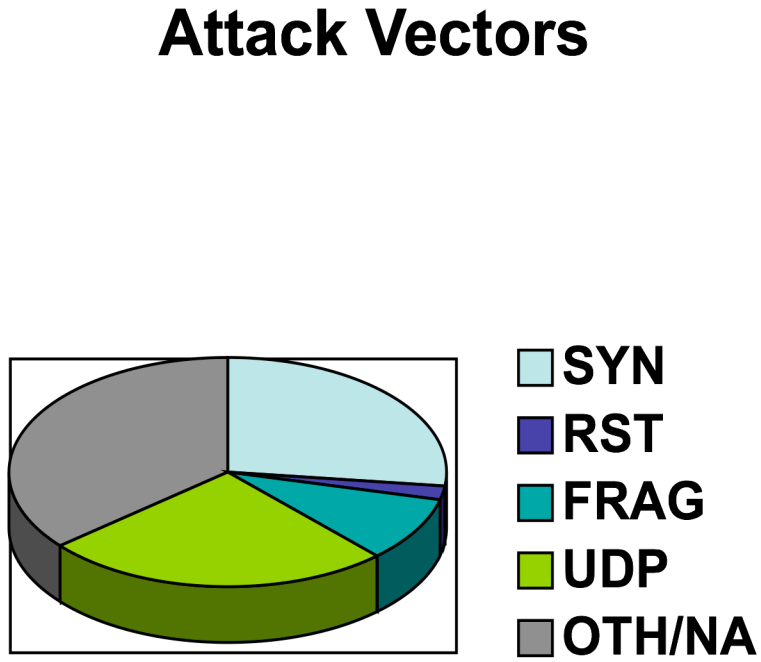
Largest Attacks Observed



10 respondents have observed attacks greater than 10 Gbps sustained (17 Gbps attack reported), an additional 25 from 1 - 10Gbps.

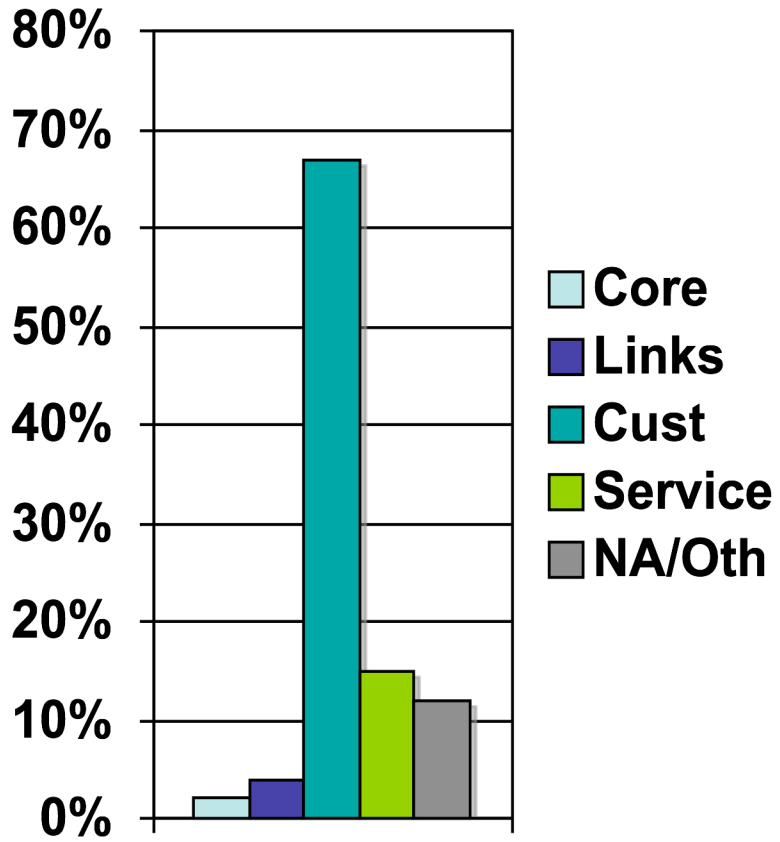
Attack Vectors

- Simple misuse “brute force” attacks still dominant
- Attacks of 14Mpps (SYN) and 22Mpps (UDP Flood) reported



Attack Targets

- Core infrastructure and customer links rarely targeted - specific customers primary target
- Services such as DNS second target of choice



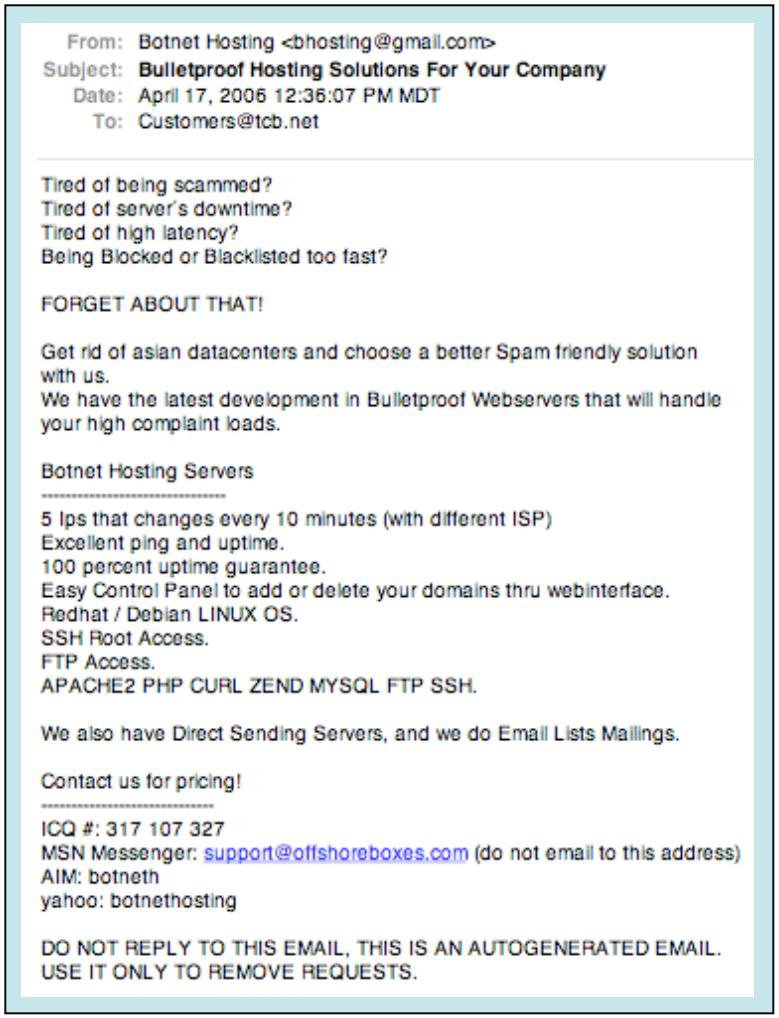
Attack Targets

- IRC/chat most common response
- Gaming servers
- Adult entertainment sites
- Gambling/Online bookmakers

- *"The kind that pay protection :-)"*

Trends in botnets

- Commonly observe 150K node botnets
- Smaller & better organized
- Better obfuscated
- More capabilities
- Using public IRC servers now
- More difficult to monitor
- More botnets - more firepower
- *“Better marketing by botherders”*



From: Botnet Hosting <bhosting@gmail.com>
Subject: **Bulletproof Hosting Solutions For Your Company**
Date: April 17, 2006 12:36:07 PM MDT
To: Customers@tcb.net

Tired of being scammed?
Tired of server's downtime?
Tired of high latency?
Being Blocked or Blacklisted too fast?

FORGET ABOUT THAT!

Get rid of asian datacenters and choose a better Spam friendly solution with us.
We have the latest development in Bulletproof Webservers that will handle your high complaint loads.

Botnet Hosting Servers
---
5 Ips that changes every 10 minutes (with different ISP)
Excellent ping and uptime.
100 percent uptime guarantee.
Easy Control Panel to add or delete your domains thru webinterface.
Redhat / Debian LINUX OS.
SSH Root Access.
FTP Access.
APACHE2 PHP CURL ZEND MYSQL FTP SSH.

We also have Direct Sending Servers, and we do Email Lists Mailings.

Contact us for pricing!

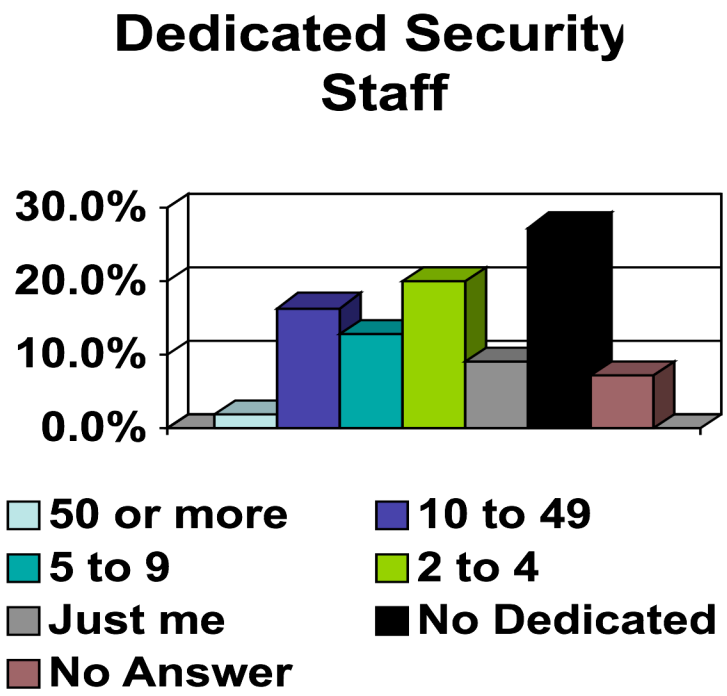
ICQ #: 317 107 327
MSN Messenger: support@offshoreboxes.com (do not email to this address)
AIM: botneth
yahoo: botnethosting

DO NOT REPLY TO THIS EMAIL, THIS IS AN AUTOGENERATED EMAIL.
USE IT ONLY TO REMOVE REQUESTS.

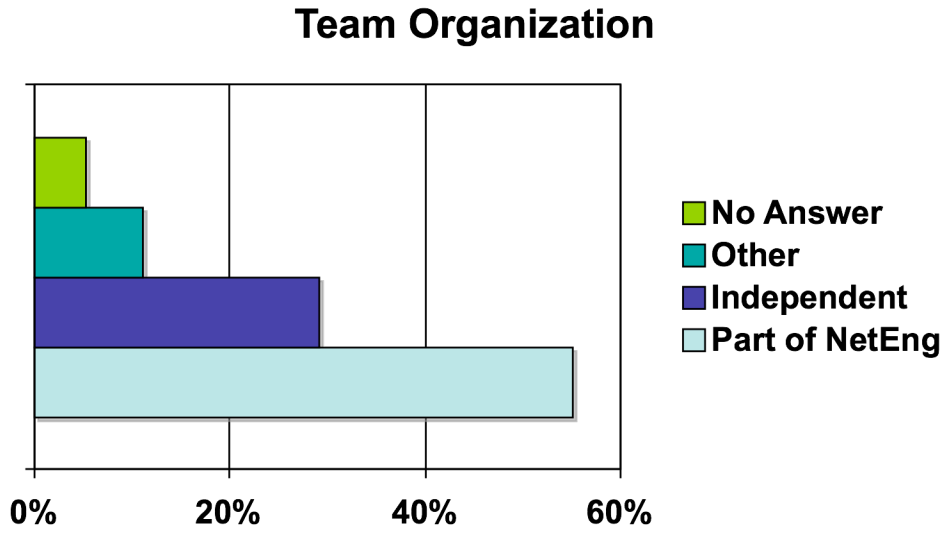
Botnet Employment

- Spamming (&& services marketing)
- [spear] Phishing
- DDOS
- ID Theft
- Form & keystroke logging
- Proxy
- Scanning
- SSH brute force attacks
- Recursive DNS/DDOS
- Think of the possibilities!

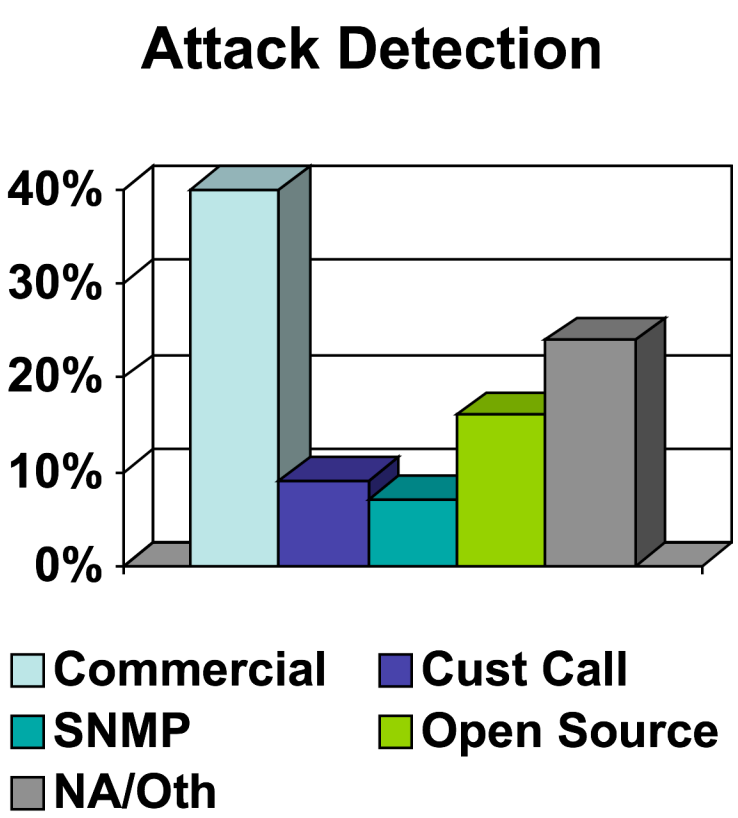
Security Organizations

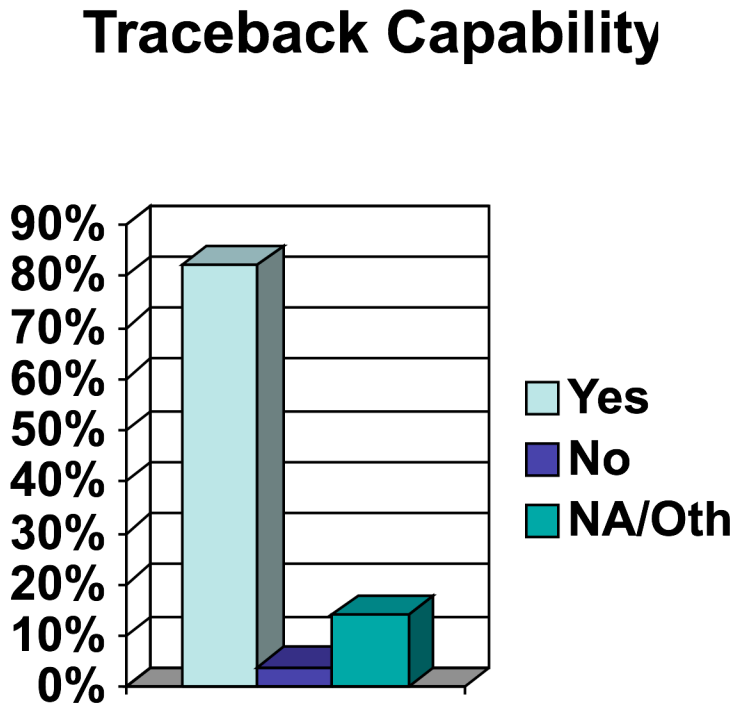


Large dedicated staff indicative of large user pool; e.g., dial-up and residential broadband services



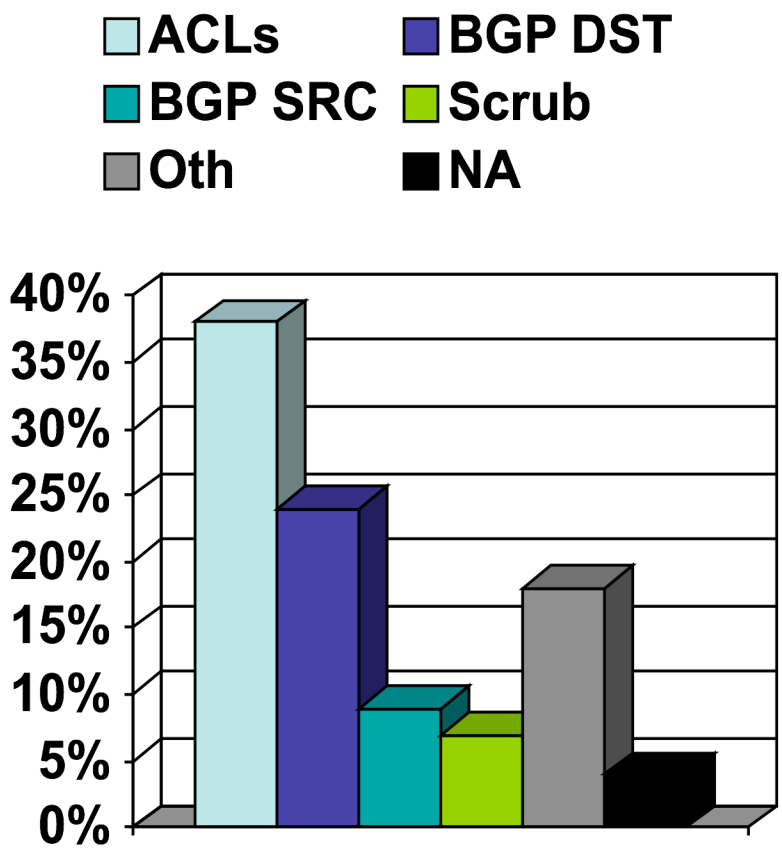
Attack Detection & Traceback





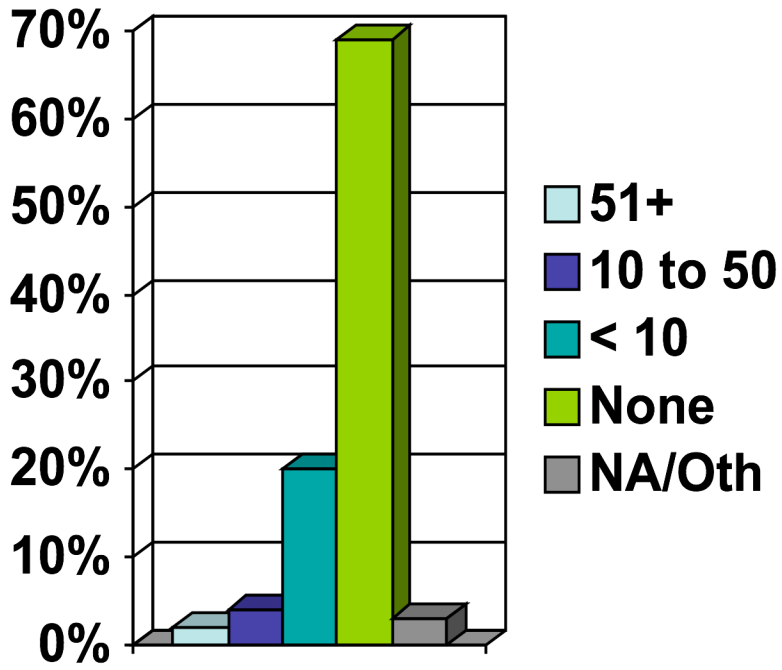
Mitigation

- ACLs are primarily destination-based with Network & Transport Layer policies
- **Number 1 & 2 techniques effectively complete DOS attack!**



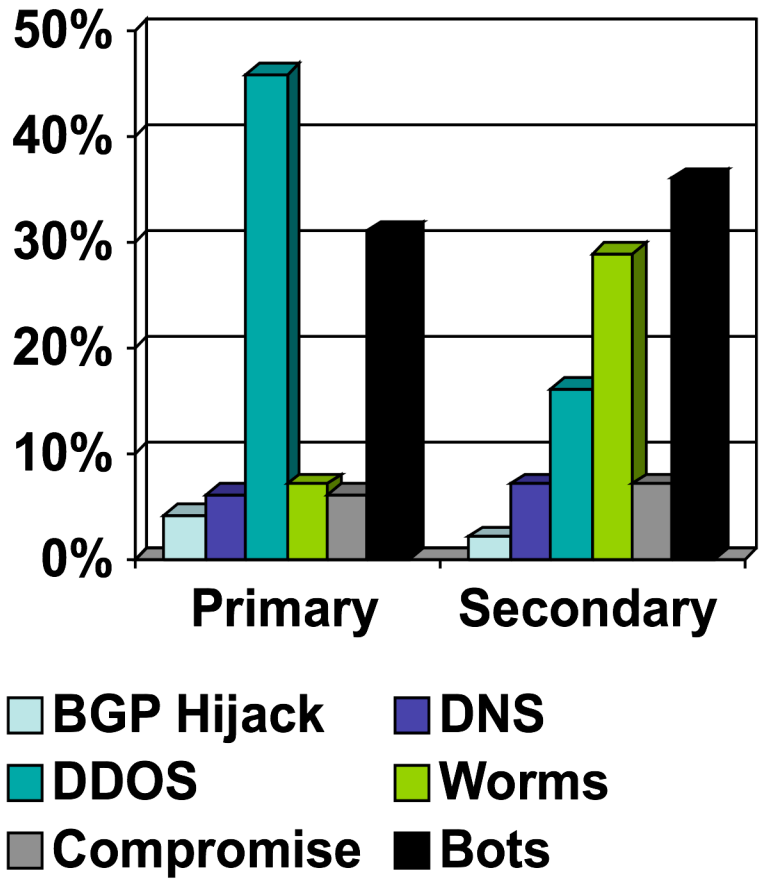
Law Enforcement Referrals

- Referrals limited by:
  - Lack of forensics detail
  - Belief in utility
  - Customer privacy request
  - Too many attacks to bother
- Only 29% of respondents believe LEOs have the power and means to to act upon information provided about attacks



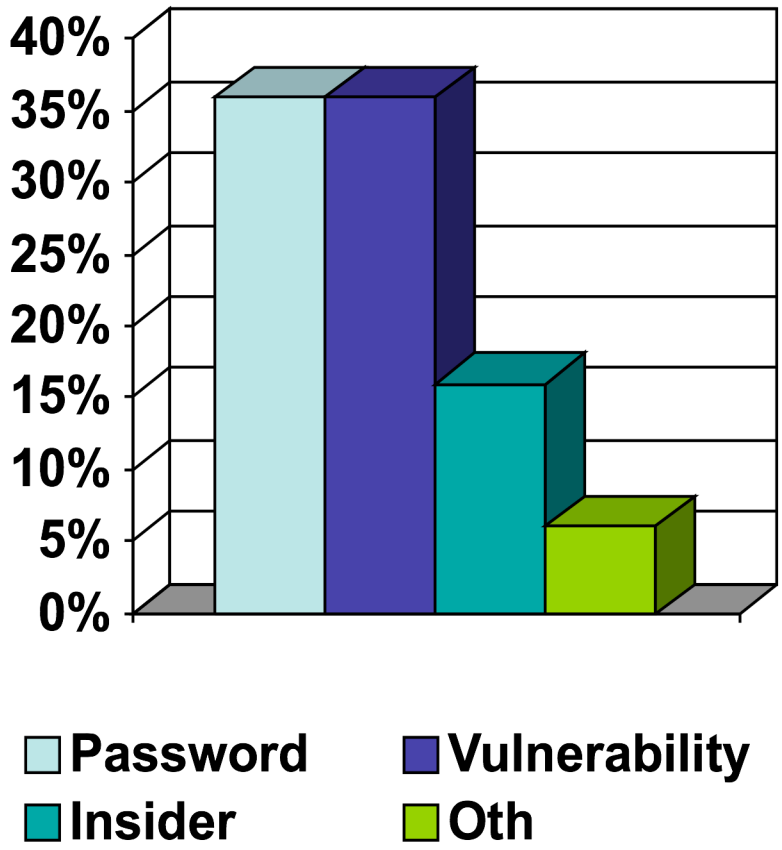
Primary Concerns

- Bots new category - most threats executed by bots
- Worm concern was implicit DDOS attributes (e.g., network congestion and control plane state)



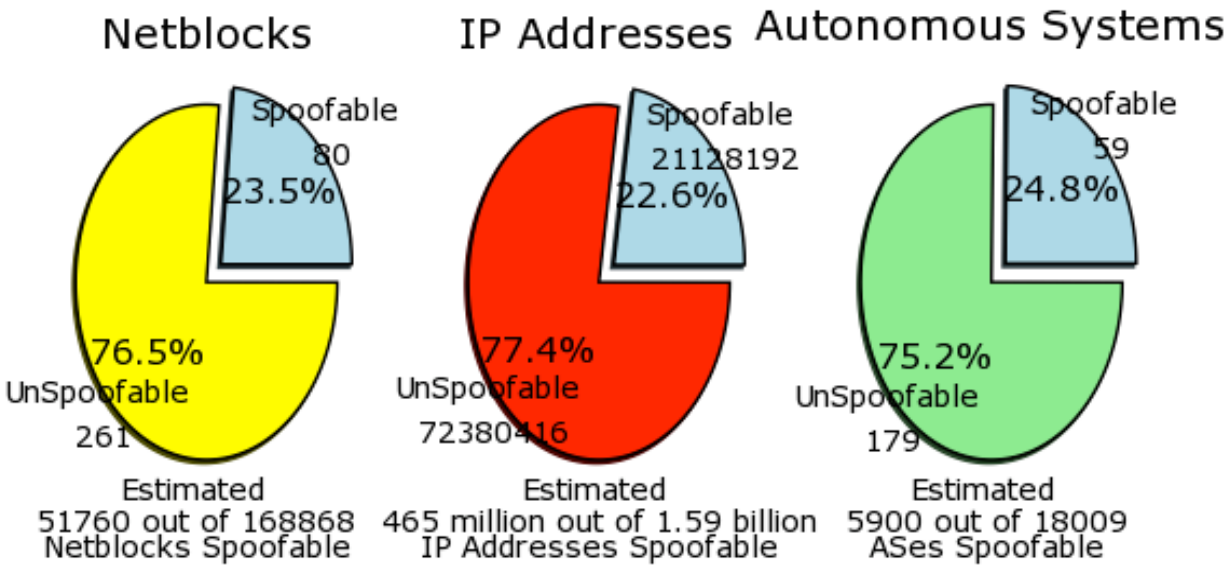
Infrastructure/OSS Attacks

- Of those respondents that have experienced internal compromise, what was the source:
  - Lack of BCP implementation
  - SNMP walk
  - Poor security practices
  - Social Engineering

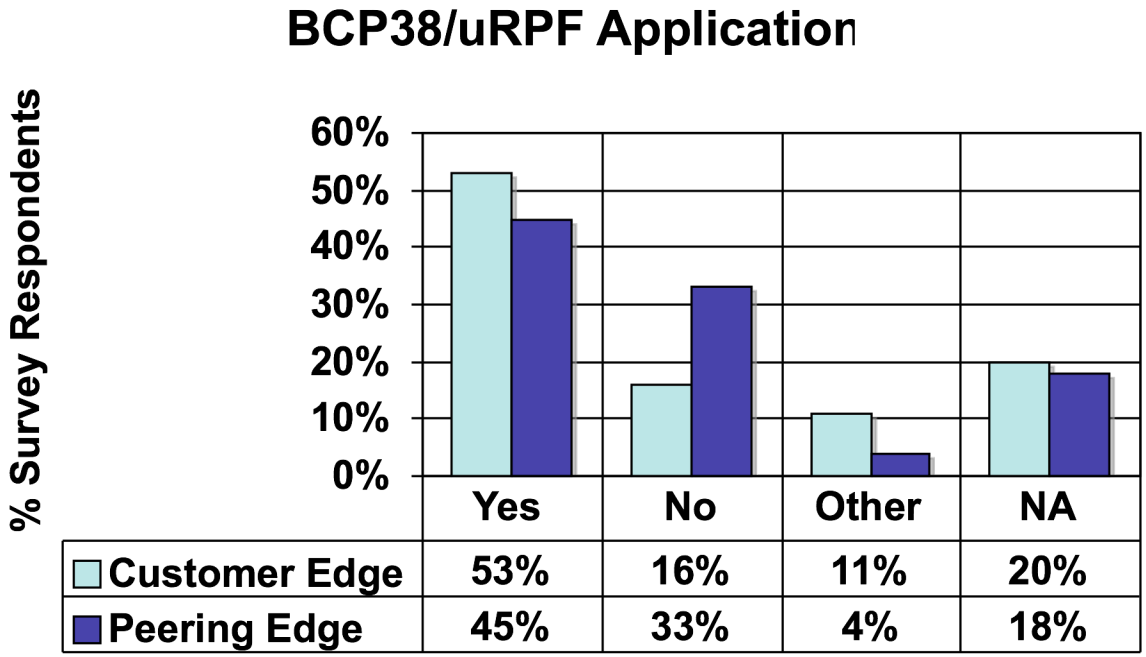


MIT ANA Spoofer Project

- http://momo.lcs.mit.edu/spoofer
- ~23% of observed netblocks corresponding to ~24% of observed ASes allow spoofing



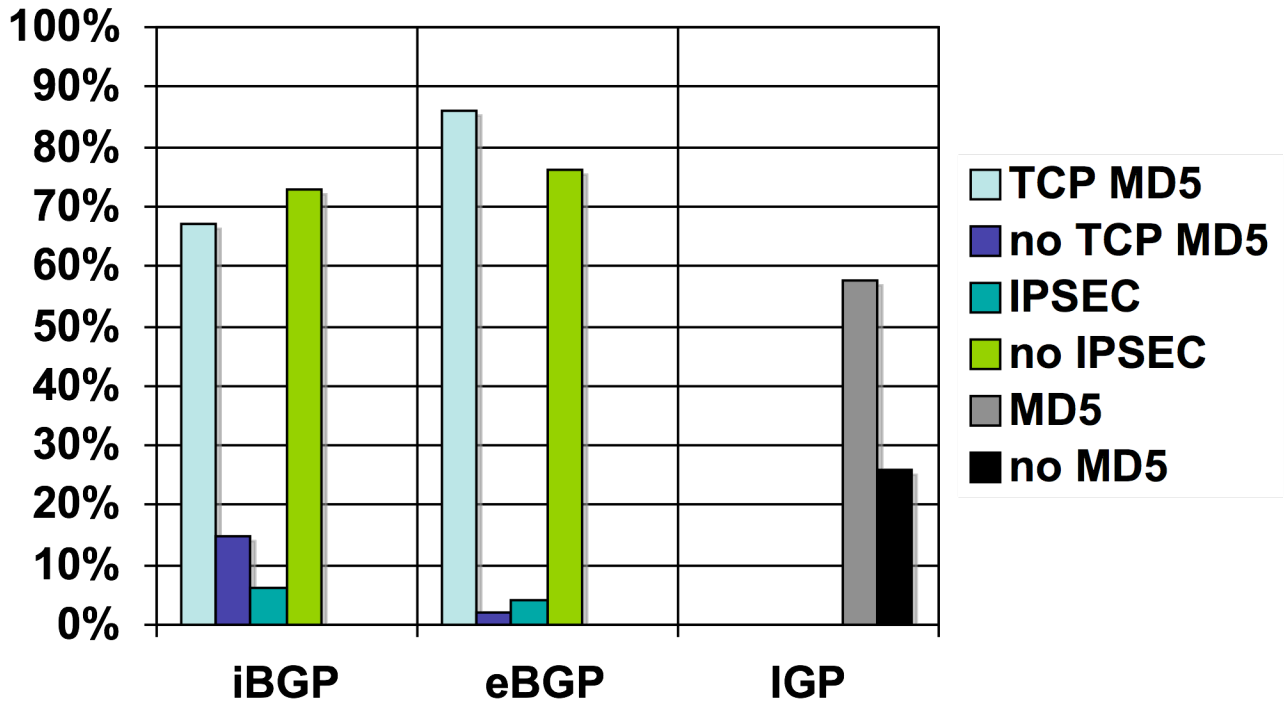
Ingress Filtering Employment



	Yes	No	Other	NA
Customer Edge	53%	16%	11%	20%
Peering Edge	45%	33%	4%	18%

Note: Assume more-clueful operators replied so “YES” number is likely much lower. Also, uRPF (loose mode) allows spoofing of “real hosts”(e.g., permits DNS amplification attacks)

BGP/IGP Transport Protection



Deployment of control plane Transport protection via commonly available mechanisms

ISPs and Future Threats

- 31% believe ISPs are NOT in a position to mitigation future Internet threats
- 69% believe are, but:
  - "Only in limited deployment for MS customers"
  - "Who else can do it - customers can't"
  - "Yes - but cost model is VERY tough"
  - "Not with today's margins"
  - "$$$"
  - "Position, yes, paid to do so - NO!"

Finally….

"Everybody's got a plan - until they get hit!"

--Mike Tyson

.. Or should I say "bit"

Questions?