ARBOR® NETWORKS

Infrastructure Security Survey

Ewerton Vieira & Danny McPherson

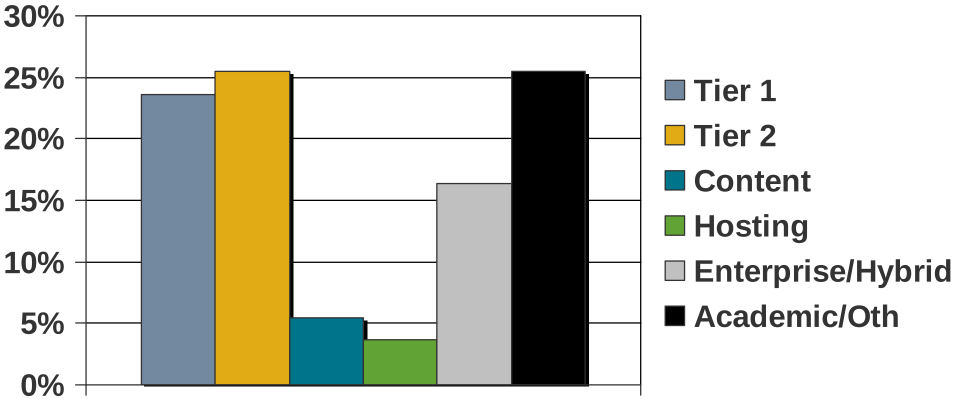
GTER 22 - Sao Paulo, Brazil

Security to the Core. Performance to the Edge.™

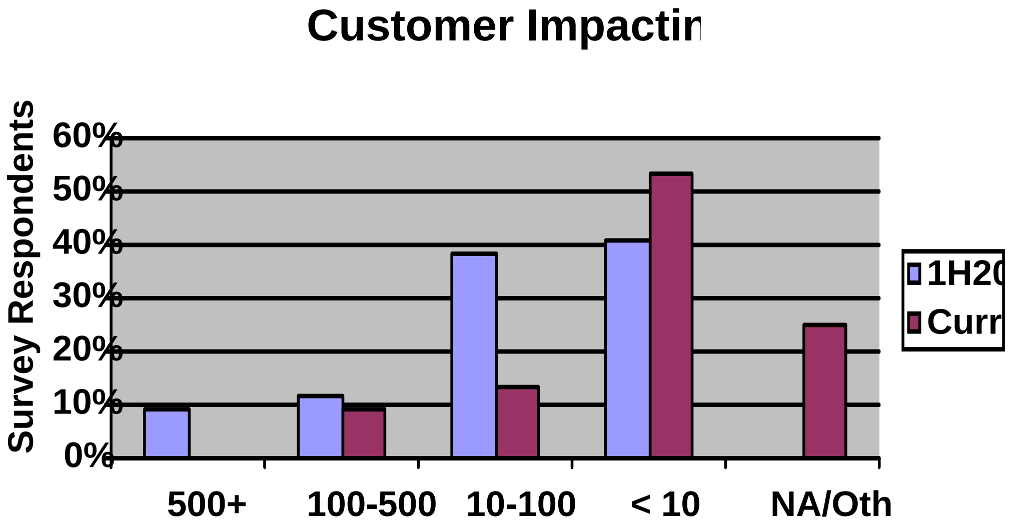
Security Survey Overview

- 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

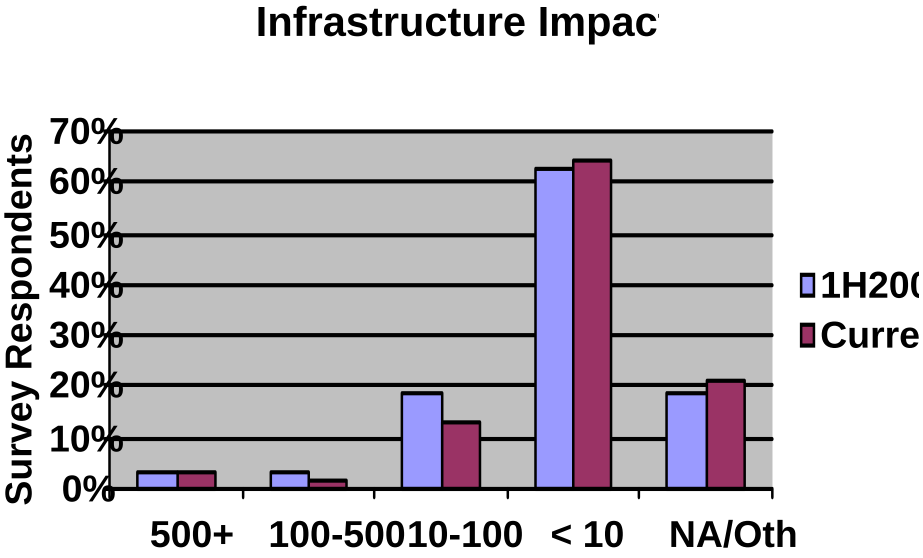
Respondent Organization Type



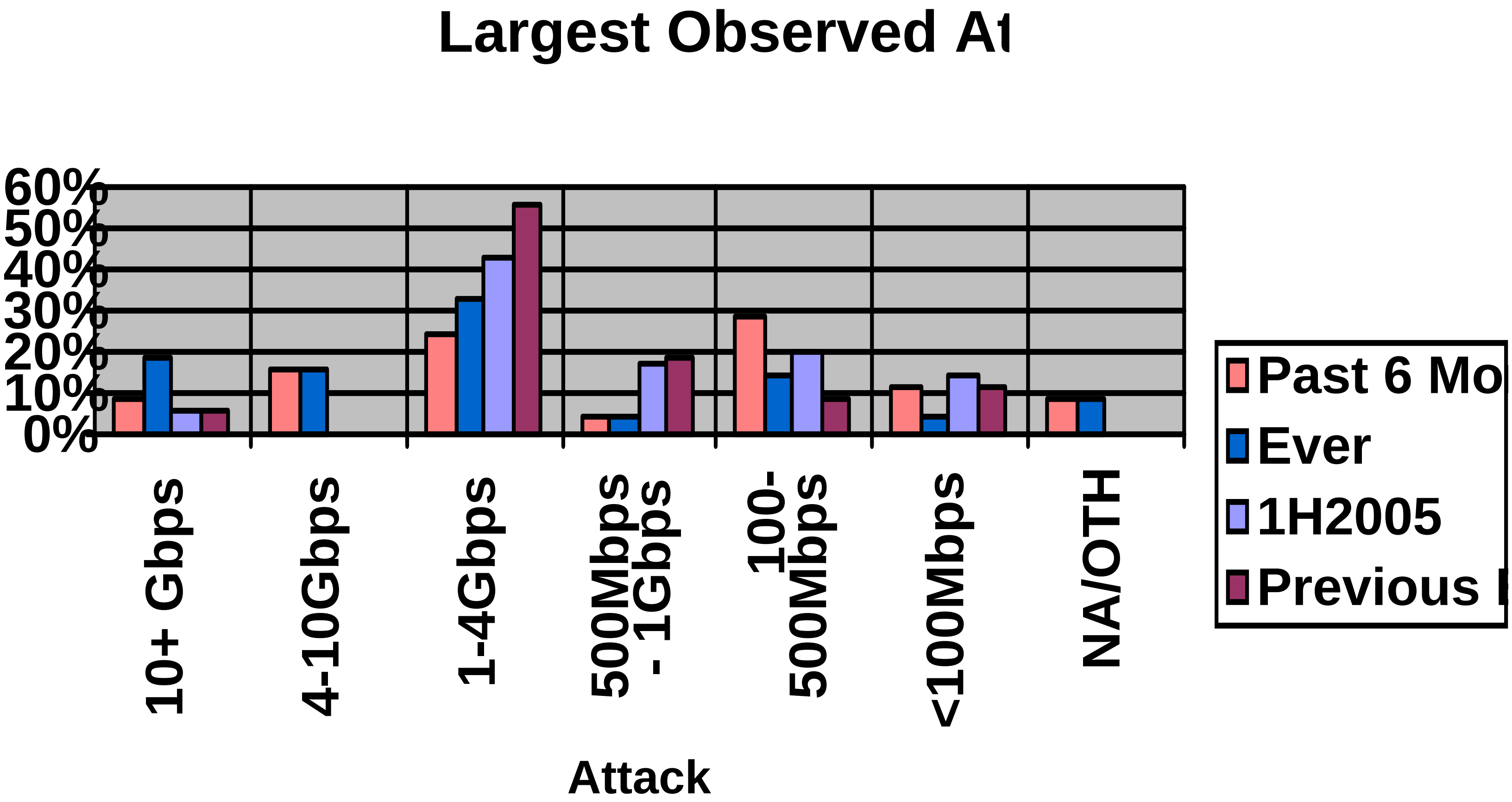
Impacting Attacks Frequency



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



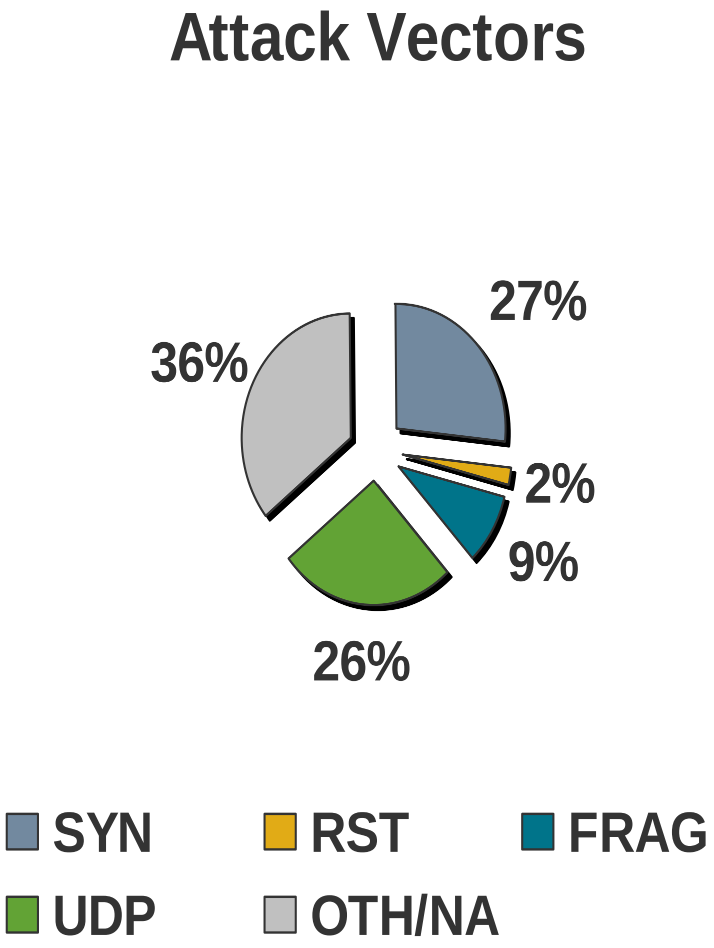
Largest Attacks Observed

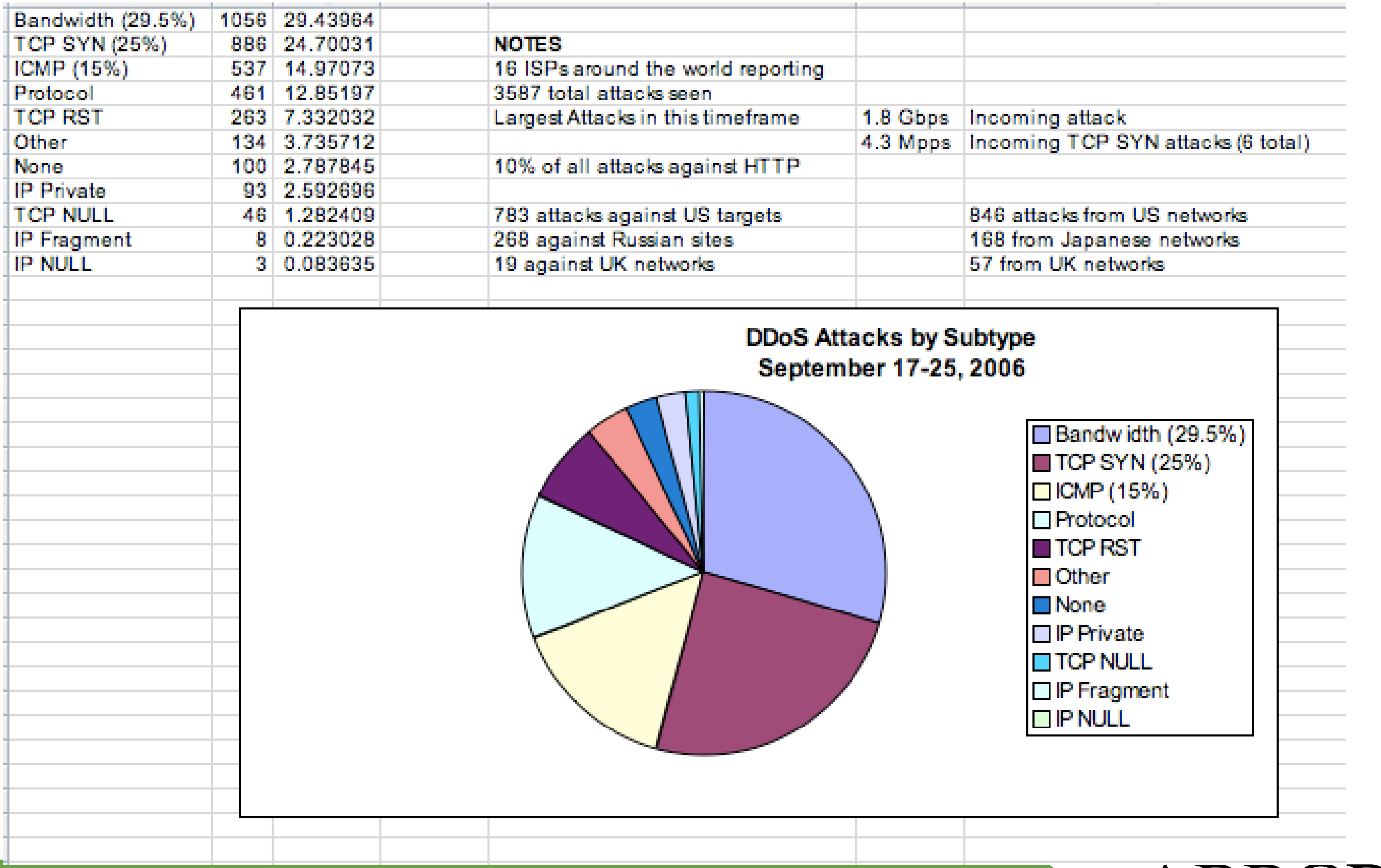


10 respondents have observed attacks greater than 10 Gbps sustained - an additional 25 from 1 - 10Gbps. Largest attack reported at 17 Gbps sustained!

Attack Vectors

- Simple misuse "brute force" attacks still dominant
- Attacks of 14Mpps (SYN) and 22Mpps (UDP Flood) reported, also 17Gbps attack reported



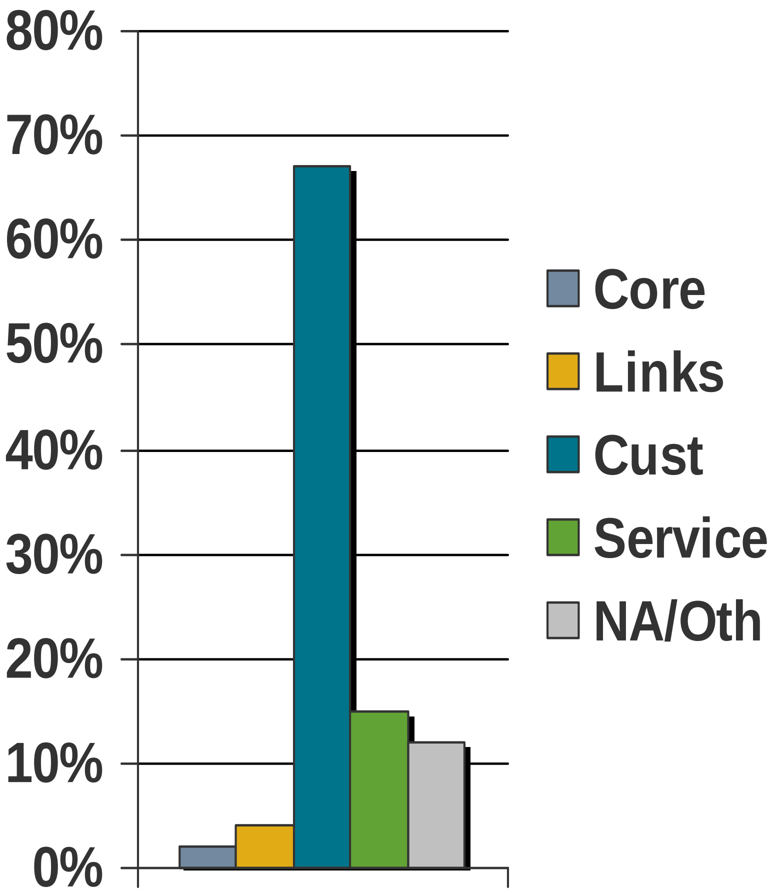


Bandwidth (29.5%)	1056	29.43964			
TCP SYN (25%)	886	24.70031	**NOTES**		
ICMP (15%)	537	14.97073	16 ISPs around the world reporting		
Protocol	461	12.85197	3587 total attacks seen		
TCP RST	263	7.332032	Largest Attacks in this timeframe	1.8 Gbps	Incoming attack
Other	134	3.735712		4.3 Mpps	Incoming TCP SYN attacks (6 total)
None	100	2.787845	10% of all attacks against HTTP		
IP Private	93	2.592696			
TCP NULL	46	1.282409	783 attacks against US targets		846 attacks from US networks
IP Fragment	8	0.223028	268 against Russian sites		168 from Japanese networks
IP NULL	3	0.083635	19 against UK networks		57 from UK networks

DDoS Attacks by Subtype
September 17-25, 2006

Attack Targets

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



Attack Targets

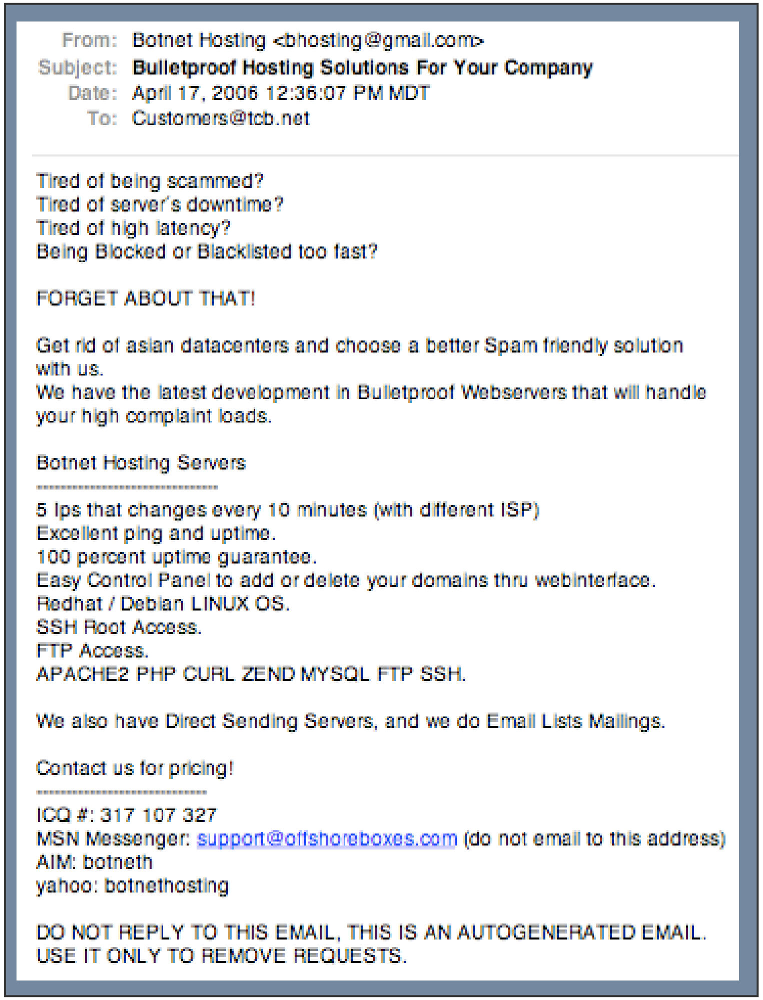
- IRC/chat most common response
- Gaming servers
- Adult entertainment sites
- Gambling/Online bookmakers
- Religious/Political

- *“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
- Click Fraud
- Scanning
- SSH brute force attacks
- Recursive DNS/DDOS

- 1.5M node botnet observed in the wild

THE WORLD'S ONLY RELIABLE NEWSPAPER

COMPUTER VIRUS SPREADS TO HUMANS!

BAR GLASSES HELP YOU SEE STRAIGHT WHEN YOU'RE DRUNK!

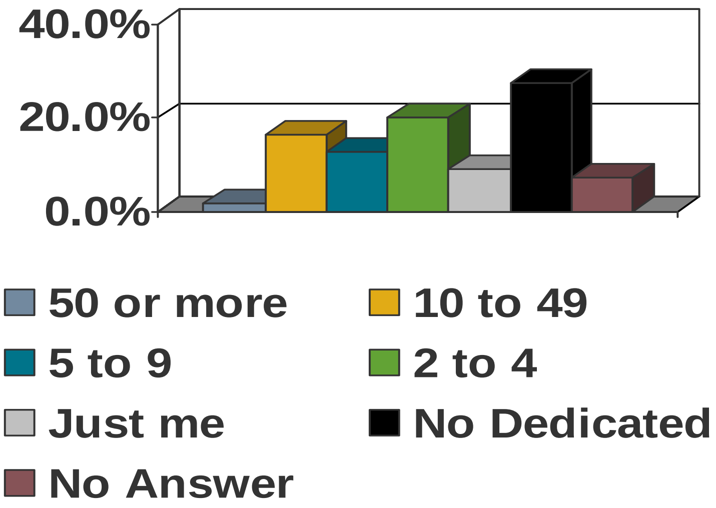
911 MISUNDERSTANDS 'BEAR WITH ME' – MAN IS MAULED

Think of the possibilities!

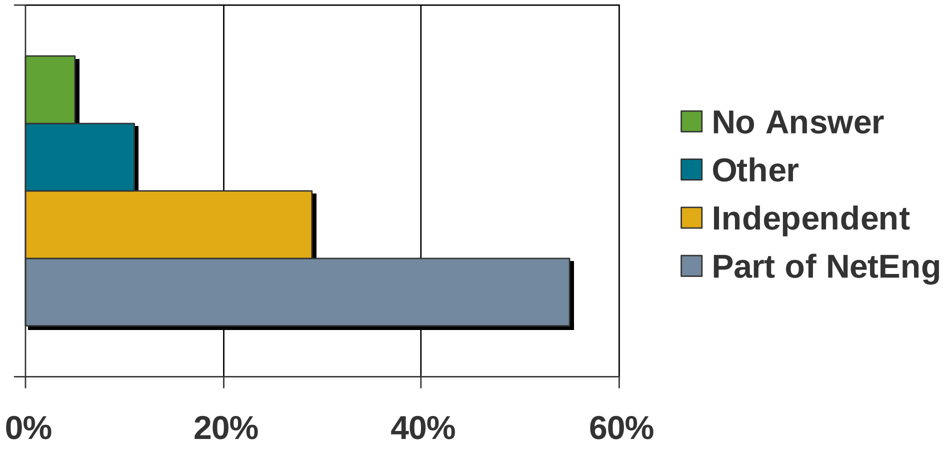
Security Organizations

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

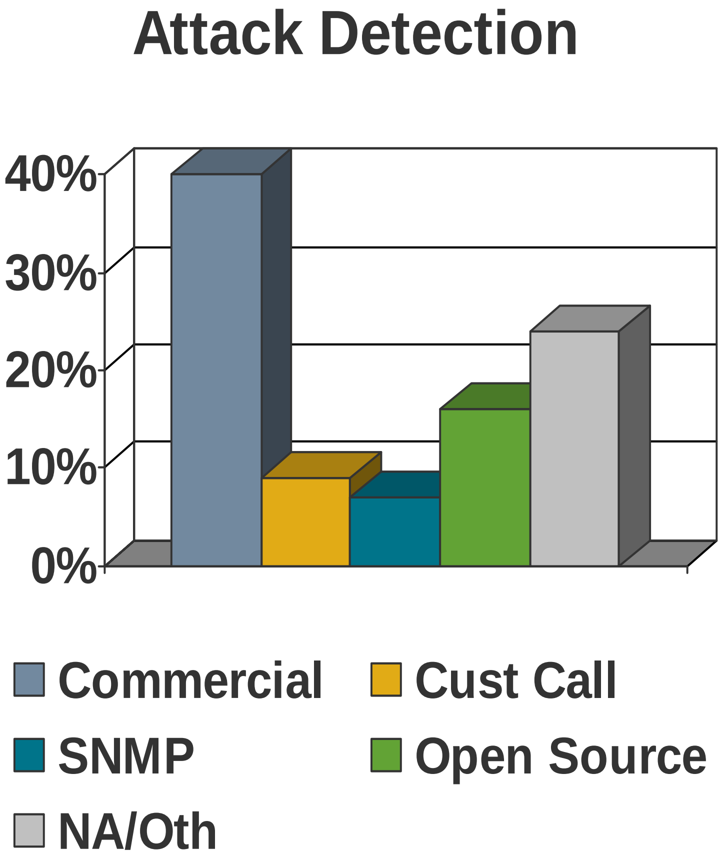
Dedicated Security Staff

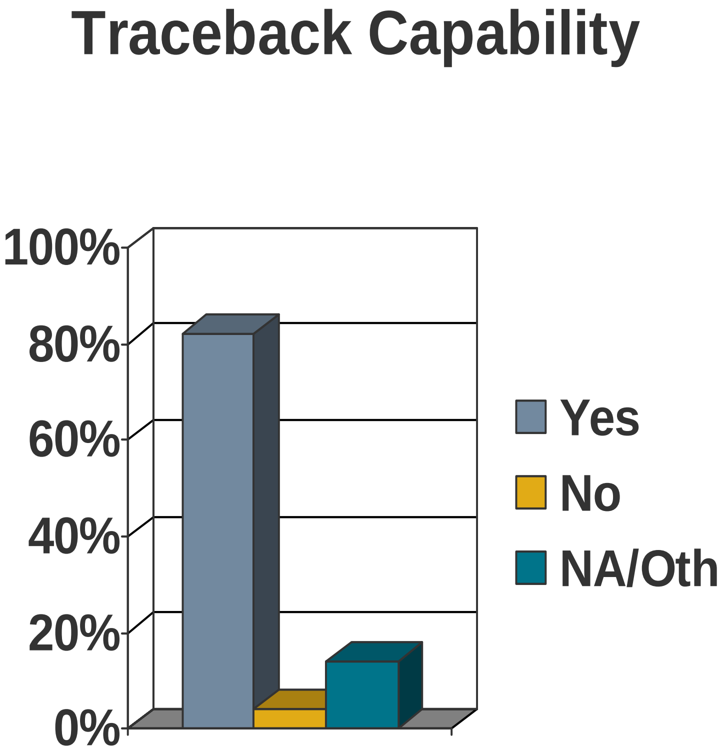


Team Organization



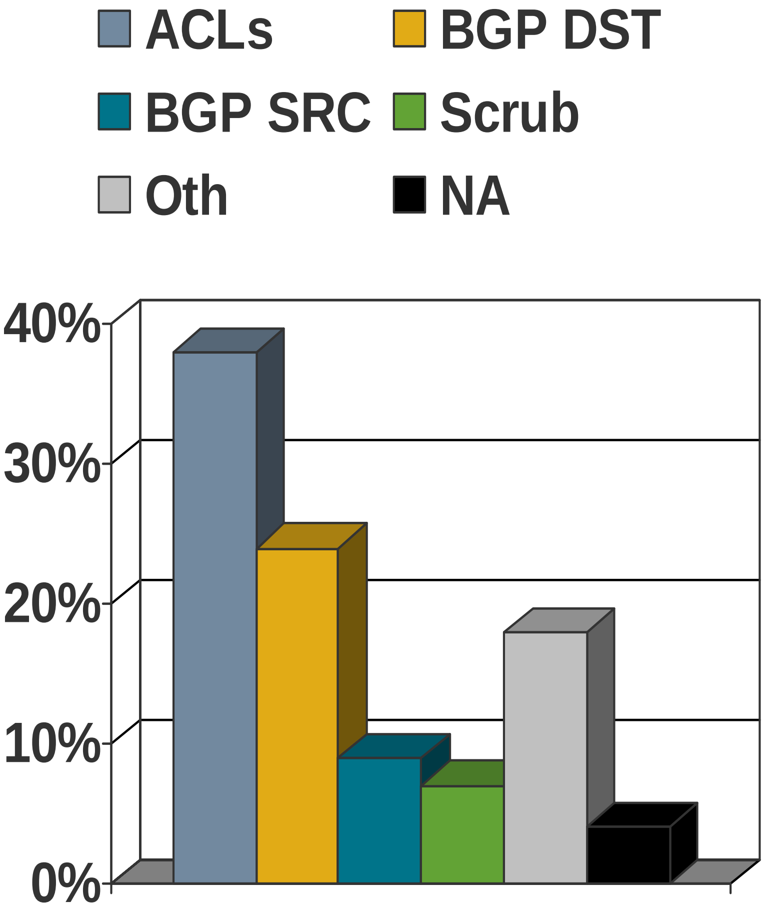
Attack Detection & Traceback





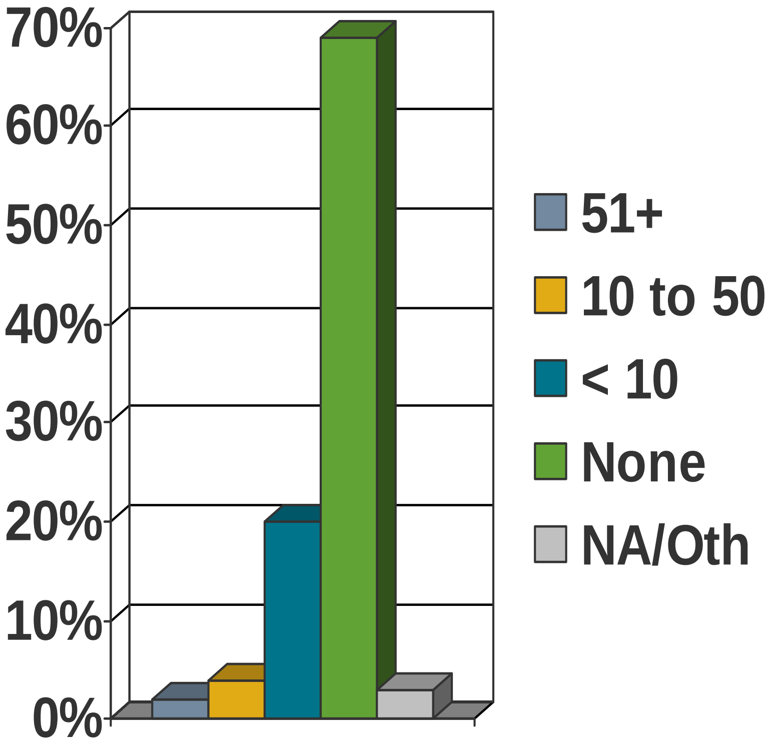
Mitigation

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



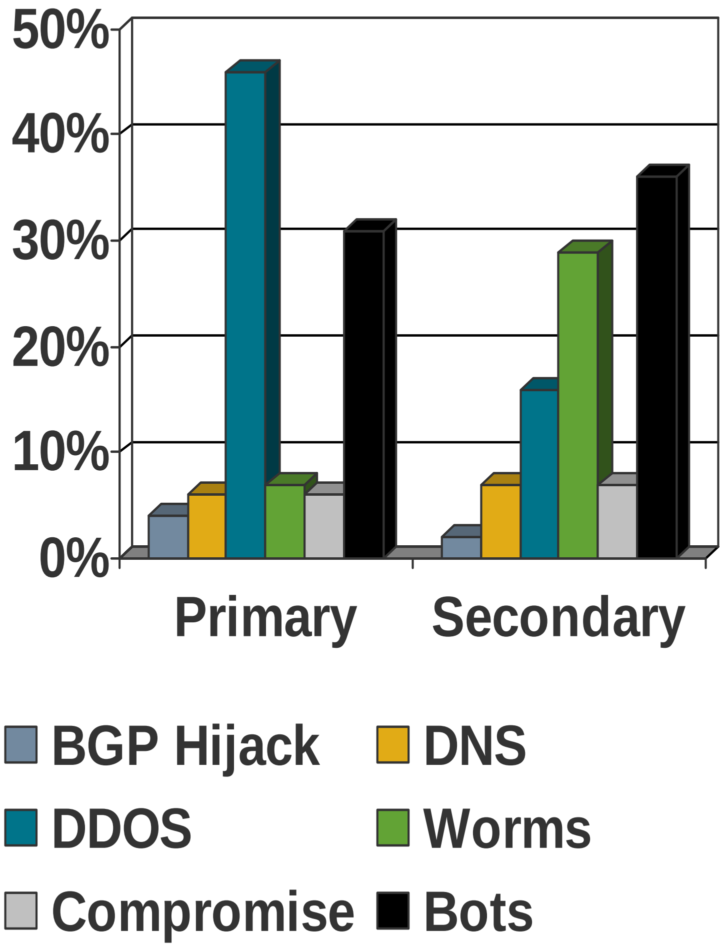
Law Enforcement Referrals

- **Less than 2% of actionable attacks referred to LEOs**
- **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 act upon information provided about attacks**



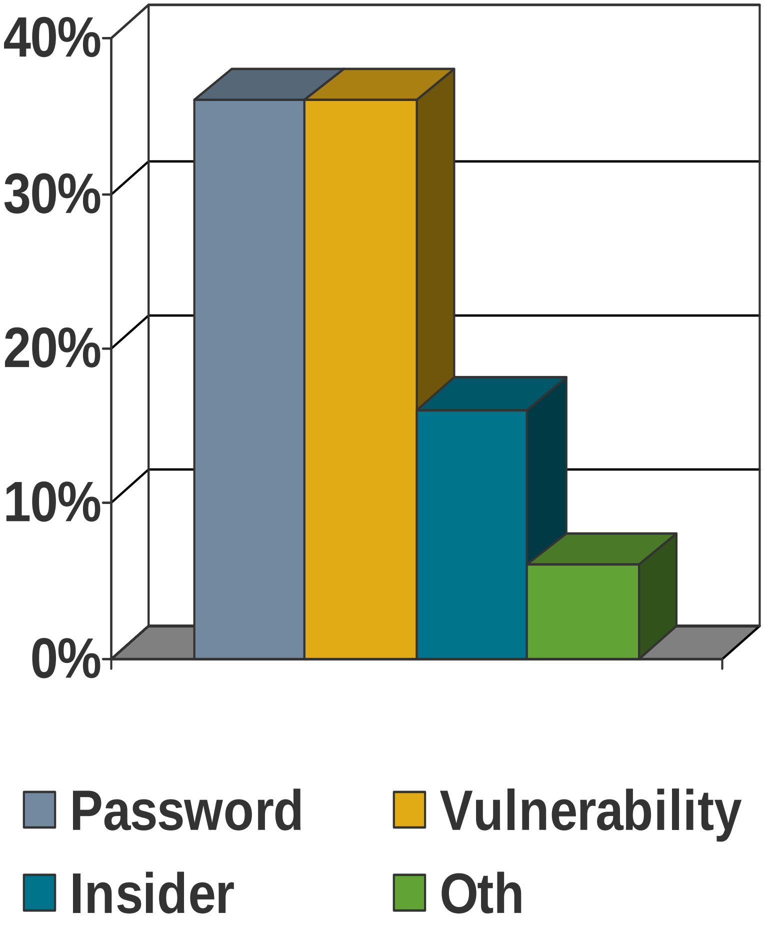
Primary Concerns

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

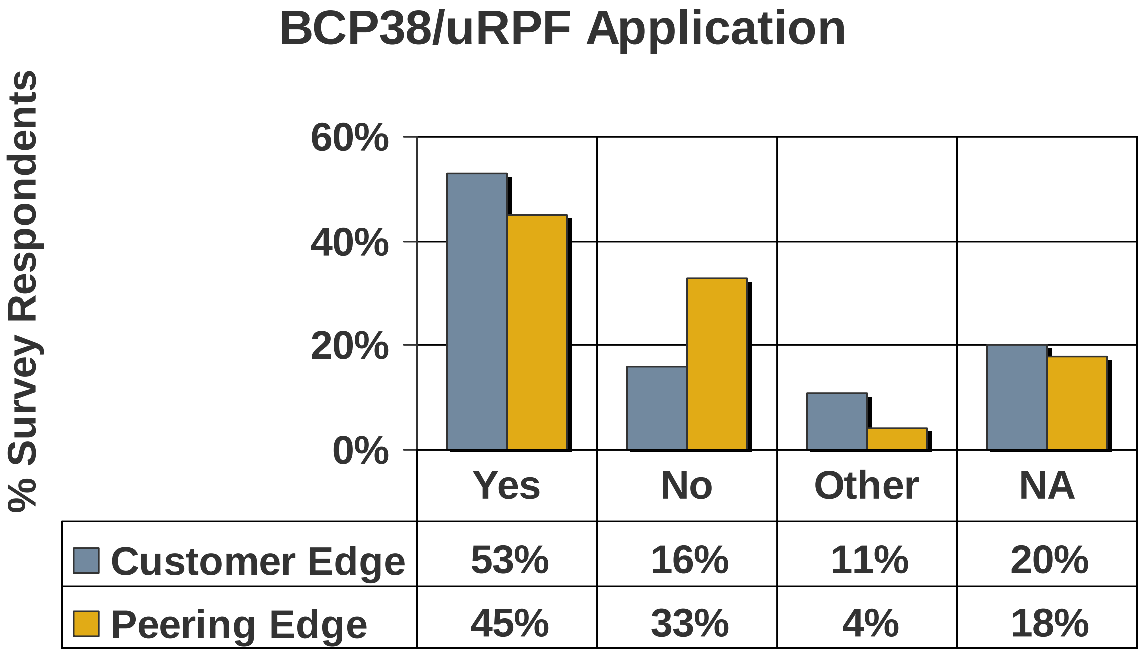


Infrastructure/OSS Attacks

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



Ingress Filtering Employment



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

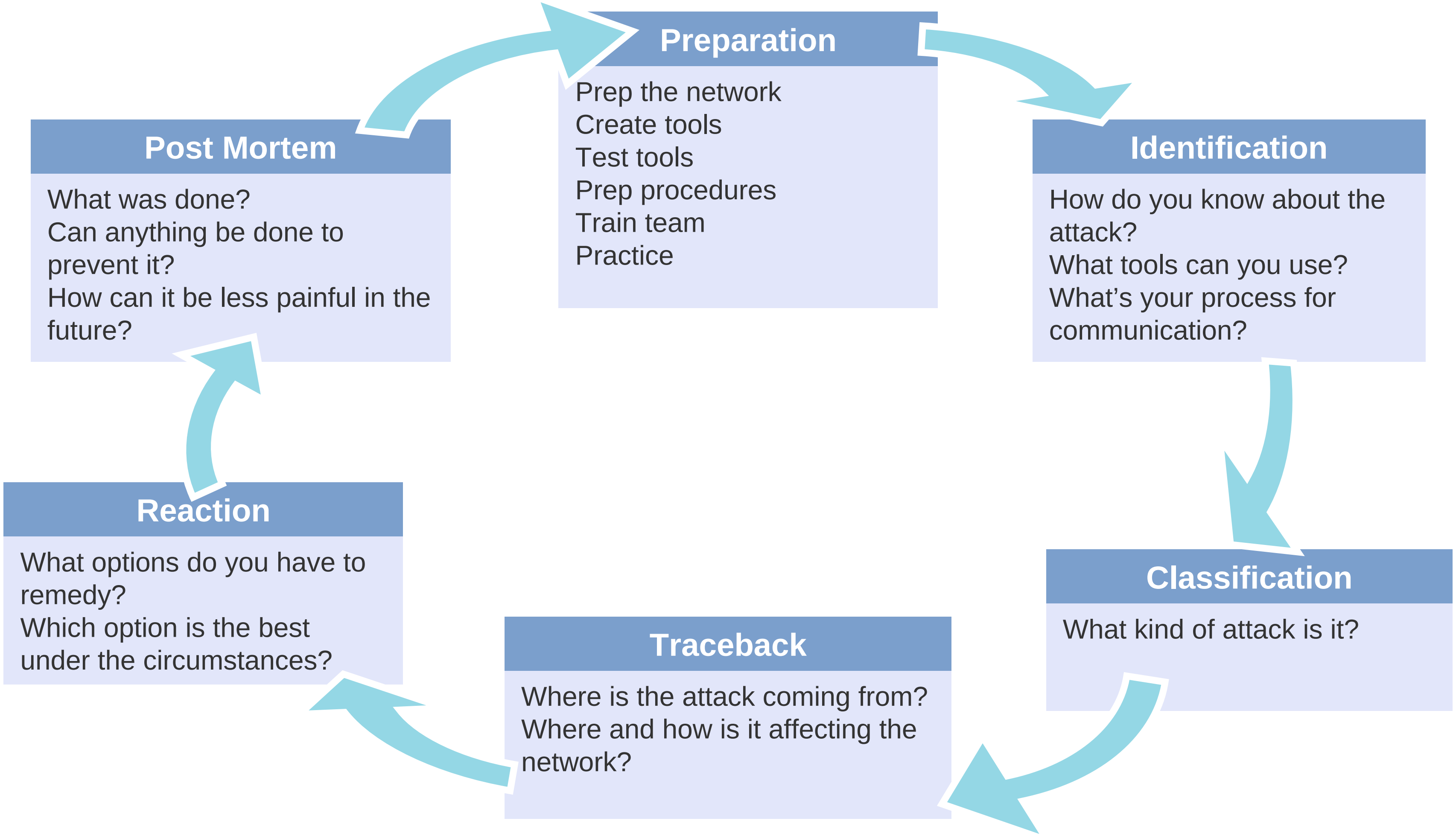
Some concern uRPF loose mode introduces false sense of protection

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)

ISPs and Future Threats

- **31% believe ISPs are NOT in a position to mitigate future Internet threats**
- **69% believe they 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!"

Six Phases of Incident Response



Preparation

Prep the network
Create tools
Test tools
Prep procedures
Train team
Practice

Identification

How do you know about the attack?
What tools can you use?
What's your process for communication?

Classification

What kind of attack is it?

Traceback

Where is the attack coming from?
Where and how is it affecting the network?

Reaction

What options do you have to remedy?
Which option is the best under the circumstances?

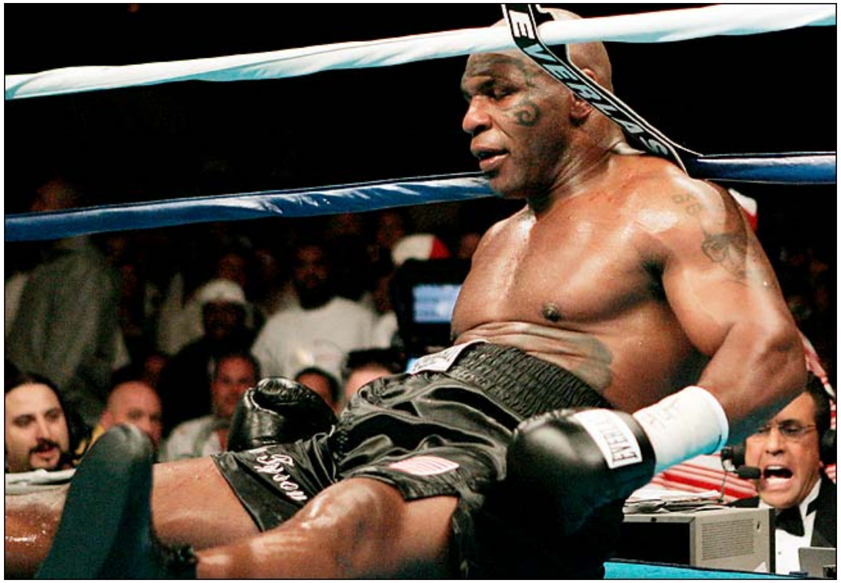
Post Mortem

What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Finally….

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

--Mike Tyson



.. Or should I say "bit"

ARBOR® NETWORKS

Thanks!

{danny,evieira}@arbor.net

Security to the Core. Performance to the Edge.™