NSP-SEC – The Details

- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC

- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
  - Multiple Layers of sanity checking the applicability and trust levels of individuals.
  - Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC-AP

- NSP-SEC-AP – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
  - Multiple Layers of sanity checking the applicability and trust levels of individuals.
  - Not meant to be perfect – just better than what we had before.

- http://puck.nether.net/mailman/listinfo/nsp-security-AP

NSP-SEC-DISCUSS

- NSP-SEC is where the mitigation takes place. You do not learn anything, you are already expected to know.
- NSP-SEC-DISCUSS (NSP-SEC-D) is the place to learn, consult, work on new mitigation techniques, and lurk (if you want to).
- http://puck.nether.net/mailman/listinfo/nsp-security-discuss

Mission Specific Groups

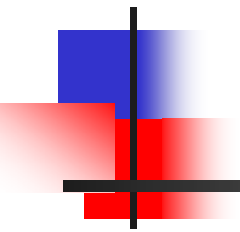
- NSP-SEC-LEO: Law Enforcement and Take Downs.
- Group of NSP-SEC members, law enforcement officers, and legal teams working on cyber-criminal take downs.

Regional Groups

- NSP-SEC-JP (Japan – In Japanese)
- NSP-SEC-BR (Brazil and other Portuguese speaking professionals)
- NSP-SEC-China (China – In Mandarin)

NSP SEC Meetings

- NANOG Security BOFs (www.nanog.org)
- RIPE Security BOFs (www.ripe.net)
- APRICOT Security BOFs (www.apricot.net)
- SANOG Security BOFs (www.sanog.org)
- And now – finally – closed door community meetings



NSP-SEC Introduction

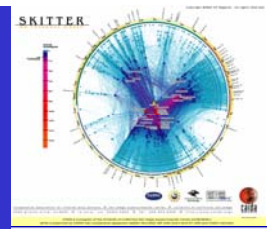
The story of the “vetted”

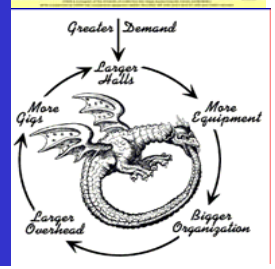
Version 1.2

Free Use

- This slide deck can be used by any operator to help empower their teams, teach their staff, or work with their customers.
- It is part of the next generation of **NANOG Security Curriculum ….** providing tools that can improve the quality of the Internet.

Overview


SKITTER


Greater Demand
Larger Halls
More Equipment
Bigger Organization
Larger Overhead
More Gigs

The Vetted – Battling the Bad Guys

WIRED MAGAZINE: ISSUE 15.09

POLITICS : SECURITY RSS

Hackers Take Down the Most Wired Country in Europe

By Joshua Davis 08.21.07 | 2:00 AM

Defense minister Jaak Aaviksoo got help from NATO in the wake of the cyberattacks. *Photo: Donald Milne*

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology d been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

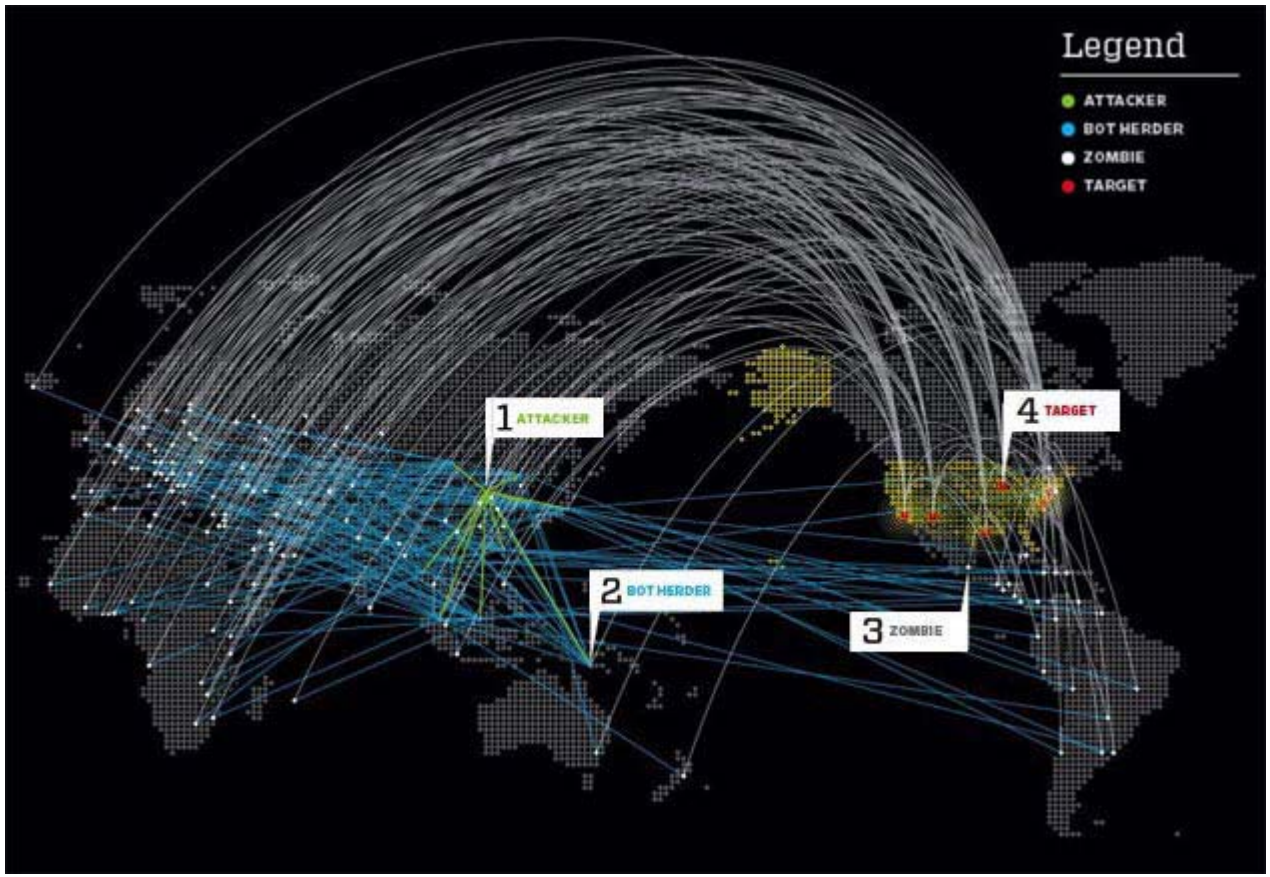
It is known as a botnet, and it had slipped into the country

FEATURE

When Bots Attack

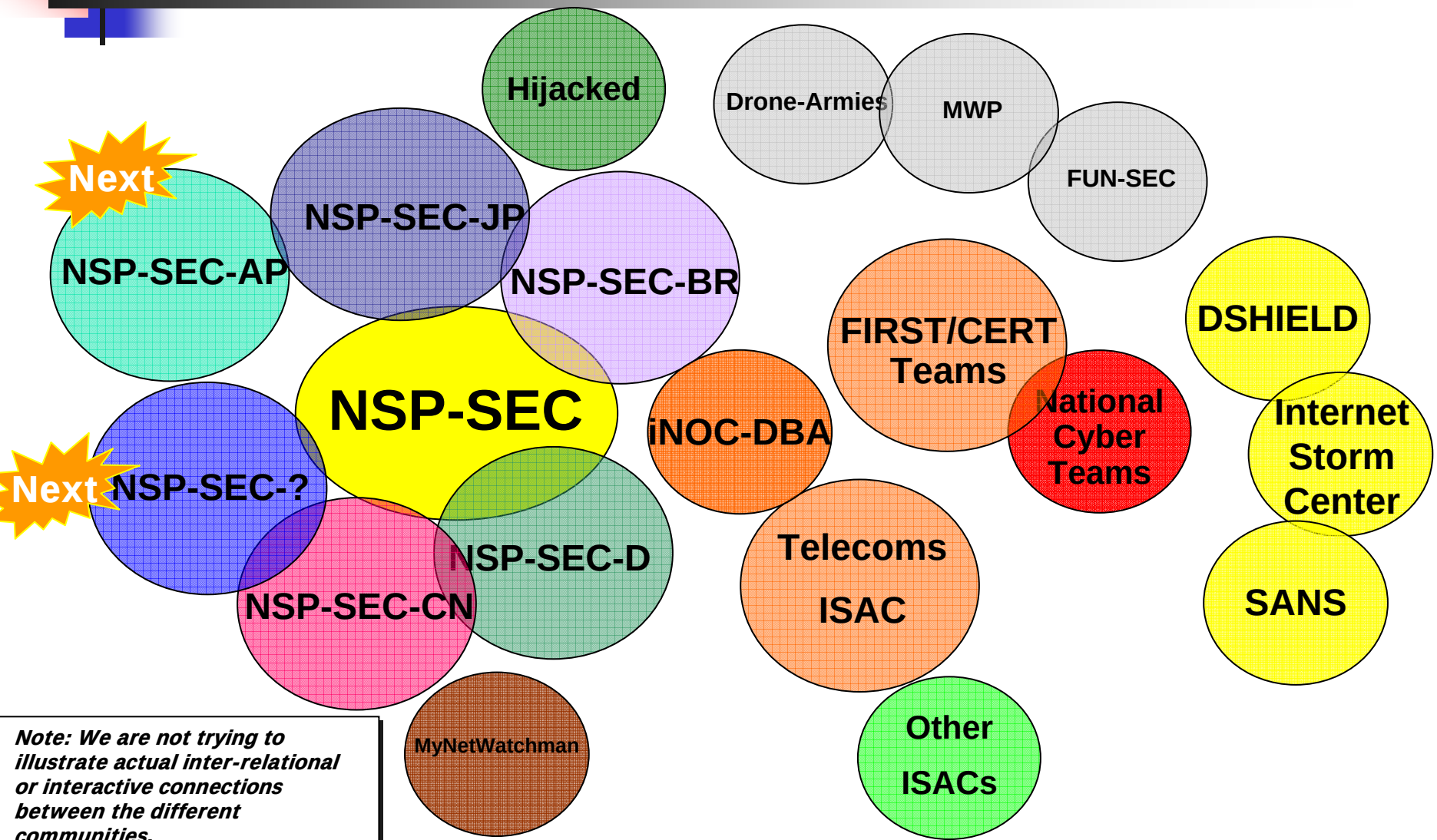
Washington Ignores

When BOTs Attack – Inter AS



http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots

Aggressive Collaboration

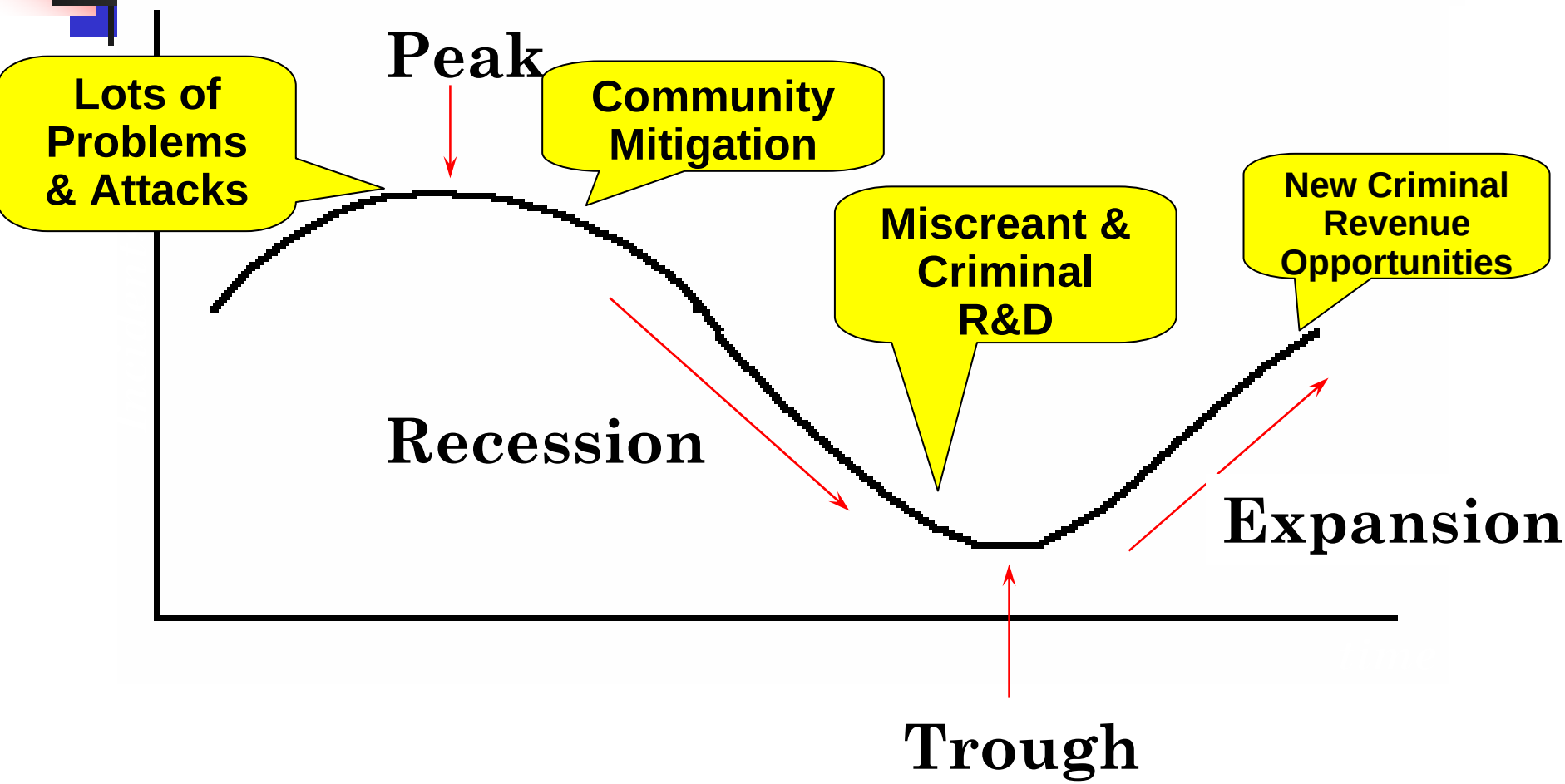


Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.

Working the 40/40/20 Rule

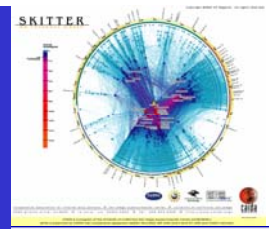
- Sean Donelan's (SBC) [sean@donelan.com] rule for end point patching:
  - 40% of the customers care and will proactively patch
  - 40% of the customers may someday care and fix/patch/delouse their machines
  - 20% of the customers just do not care and have never responded to any effort to fix them.

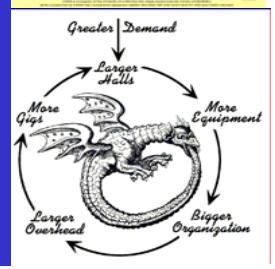
Economic Cycles



Parts of the Cyber Crminal Business Cycle

NSP-SEC

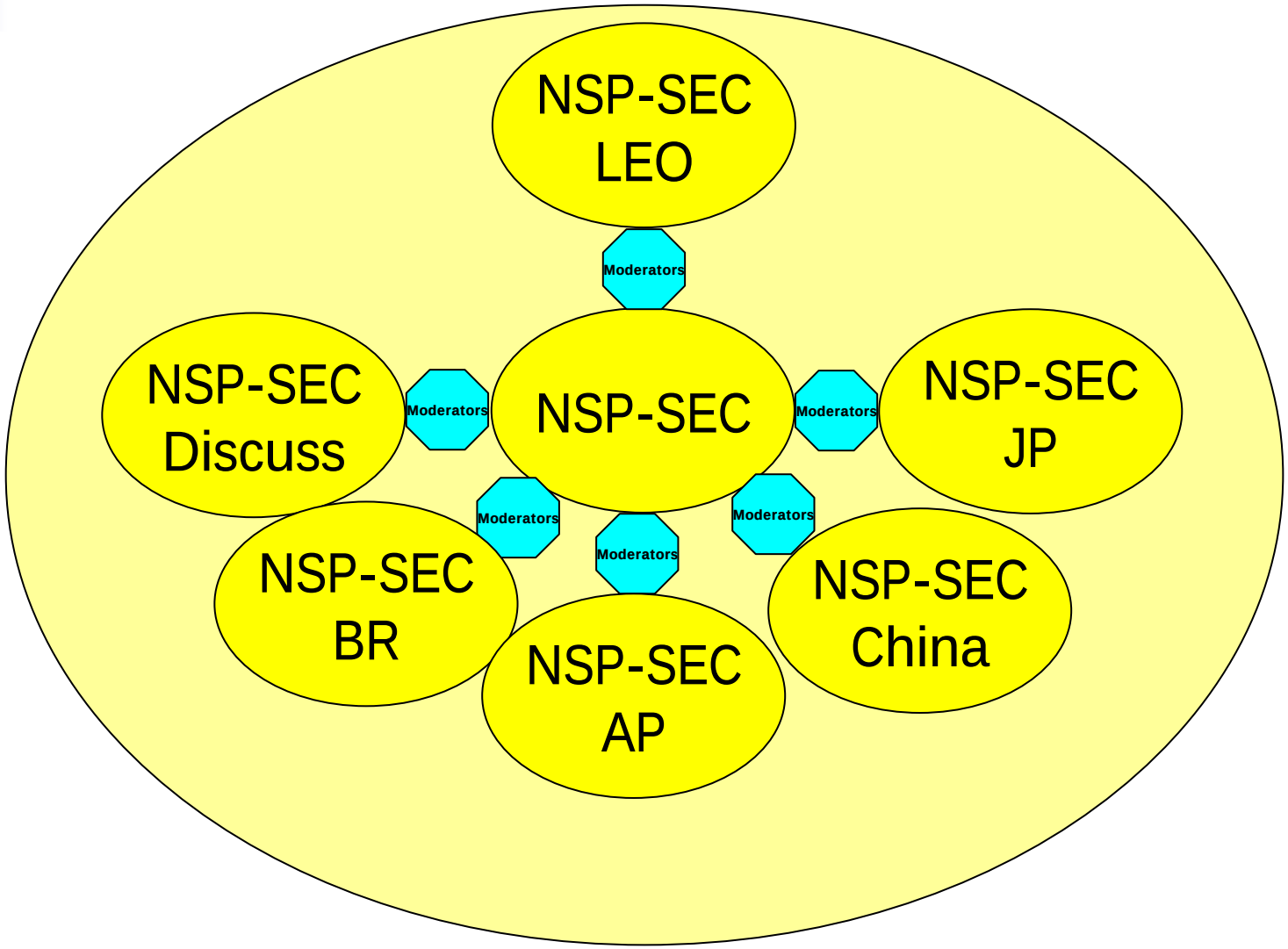

SKITTER


Greater Demand
Larger Halls
More Equipment
Bigger Organization
Larger Overhead
More Gigs

NSP-SEC's Core Function

- Protect the Critical Commercial Telecommunications Infrastructure
- Proactively and Reactively Disrupt Cyber Criminal Activities which could threaten Telecommunications Businesses
- Collaborate to restore Telecommunications Services during a Internet wide Security Incident.

NSP-SEC Multiple Communities



NSP-SEC Multiple Communities

- **NSP-SEC** (English) Proactive and Reactive Action
- **NSP-SEC-Discuss** (English) Proactive Consultations, Planning, and Tools Development.
- **NSP-SEC-LEO** (English) Global Law Enforcement Consultation and Coordination
- **NSP-SEC-JP** (Japanese) NSP-SEC Team focused on Japan's Internet Infrastructure consulting in Japanese.
- **NSP-SEC-BR** (Portuguese) NSP-SEC Team focused on Brazil's Internet Infrastructure consulting in Portuguese.
- **NSP-SEC-China** (Chinese) NSP-SEC Team focused on China's Internet Infrastructure consulting in Chinese.
- **NSP-SEC-AP** (English) NSP-SEC Regional Team focused on Internet Infrastructure in the Asia Pacific Region.

Daily NSP-SEC Activities

- Anti-BOTNET Action. Find, track, disrupt, take down, and (sometimes) assist Law Enforcement actions.
- Emerging Malware and Criminal Threats. Monitor, analyze, determine how to disrupt, map economic cycle, and plan mitigation.
- Find peers in other SPs and Law Enforcement which can assist with criminal incidents targeted directly an the SP's business.
- Collect information on all violated and infected computers on the Internet, providing details by Autonomous System Number (ASN) to each participating SP.
- Work together to coordinate responses to attacks and incidents.
- And much more ....

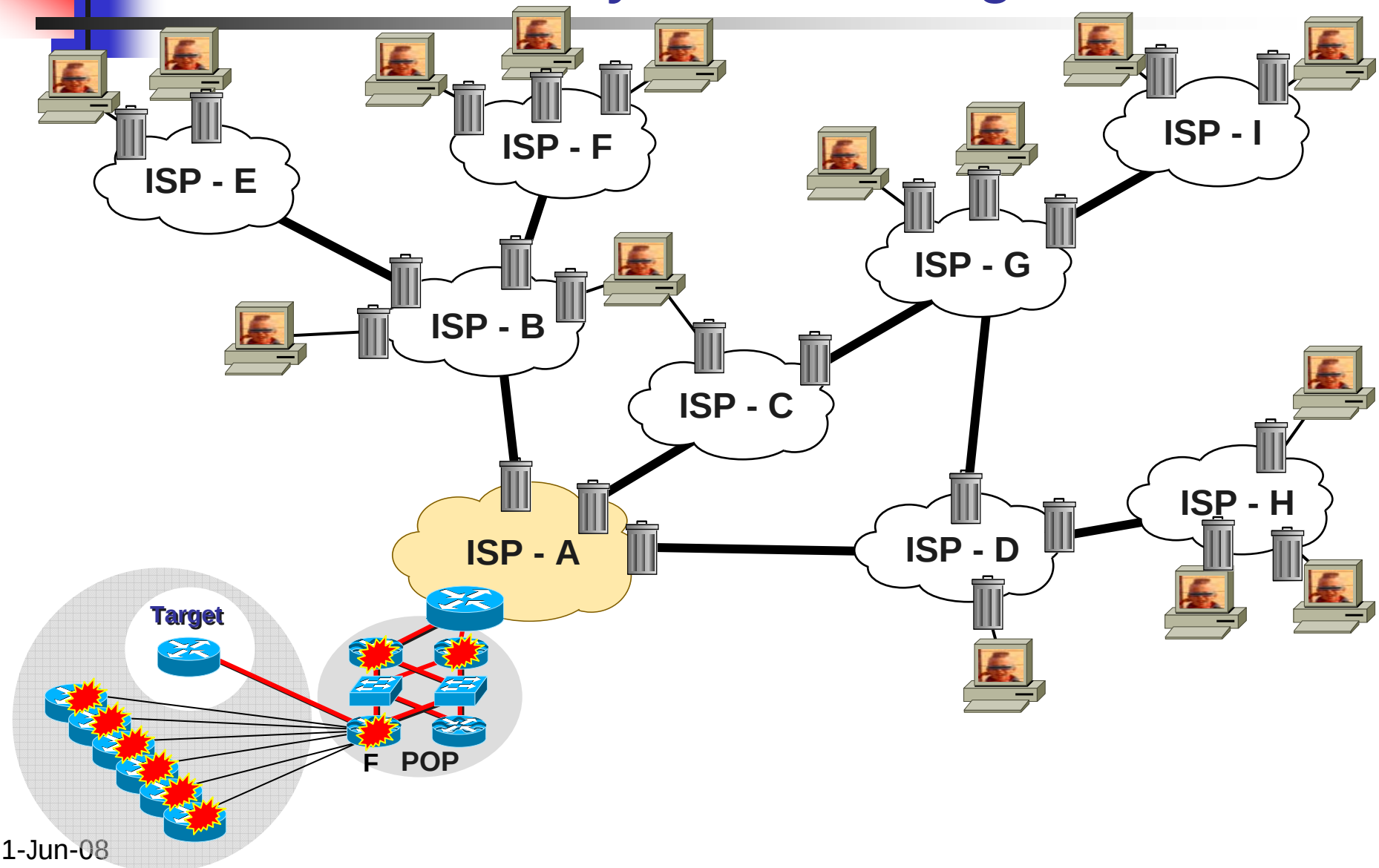
NSP-SEC: Daily DDOS Mitigation Work

I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

NSP-SEC: Daily DDOS Mitigation Work



Why be a member of the NSP-SEC Community?

- The critical industry lead organization created to protect the Internet backbones.
- Ability to find the key peers in other SPs to enable joint law enforcement action.
- The ability to have a complete list of violated/infected customer systems.
- The ability to initiate joint action to protect key SP's infrastructure and customers.

Why Haven't I Heard About NSP-SEC?

- NSP-SEC's policy is to not hide – but not broadcast to the world that it exist.
- The full capabilities of this community is not know outside of the vetted members.
- It IS THE #1 group silently disrupting the criminal enterprises. That means it cost a criminal enterprise financial gain – which from a organized crime point of view – is something that needs to be "taken care of."

It is all about *Operational Trust*

- Inter-Provider Mitigation require operation trust.
  - You need to trust your colleagues to keep the information confidential, not use it for competitive gain, not tell the press, and not tell the commercial CERTS and *Virus* circus.
  - So all membership applications are reviewed by the NSP-SEC Administrators and Approved by the membership.
  - All memberships are reviewed and re-vetted every 6 months – letting the membership judge their peer's actions and in-actions.

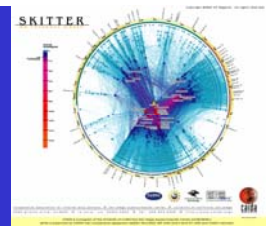
NSP-SEC is not ….

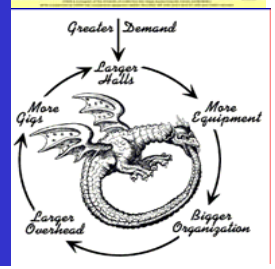
- NSP-SEC is not perfect
- NSP-SEC is not to solve all the challenges of inter-provider security coordination
- NSP-SEC is not the *ultimate solution.*
- *But NSP-SEC does impact the security of the Internet:*
  - Example: Slammer

NSP-SEC is Decentralized by Design!

- Who *owns* NSP-SEC?
  - The collective industry membership by their consensus.
- Who *runs* NSP-SEC?
  - Volunteer who have real ISP Security and Backbone engineering jobs.
- Who provides the *resources* for NSP-SEC?
  - The individual members – using their own equipment, bandwidth, and connections.

NSP-SEC History





2002 - The *Real* Security Problem

- September 2002 ISP/SP Operations Security Engineers could not:
  - Find their *security* colleagues in their directly attached peers.
  - Find security engineers in providers two hops away.
  - Find any security engineers in the big Asia providers.
- So if big attacks happened, there was no way for the people who needed to work with each other to find each other ... let alone work collectively to mitigate the attack.

2003 – A Year of Difference

- September 2003 ISP/SP Operations Security Engineers can:
  - Find their *security* colleagues in their direct peers and a huge range if global ISP/SPs.
  - Work with each other via E-mail, chat, iNOC Phone, and POTs to collectively mitigate attacks and incidents on the Internet.
  - Execute Inter-provider Tracebacks and Mitigation.
  - Proactive measures to prepare for projected attacks.
- What changed?

NSP-SEC

- NSP-SEC was created by several ISP/SP Security Engineers as a means to meet the following objectives:
  1. Provide a means for ISP/SP Security Engineers to find their colleagues.
  2. Create a potential forum for ISP/SP Security Engineers to work on DOS attacks, Incidents, and other activities.

Finding their Colleagues was the Key

- We know that:
  - Two engineers working together to mitigate an incident is more effective than one engineer working alone.
  - Incident mitigation is faster if engineers can communicate with each other during an incident.
- NSP-SEC provides that means to find colleagues and perhaps – work on the incidents.
  - It is not the exclusive mode of collaboration. “Point to Point” collaboration outside of NSP-SEC does happen and is strongly promoted.

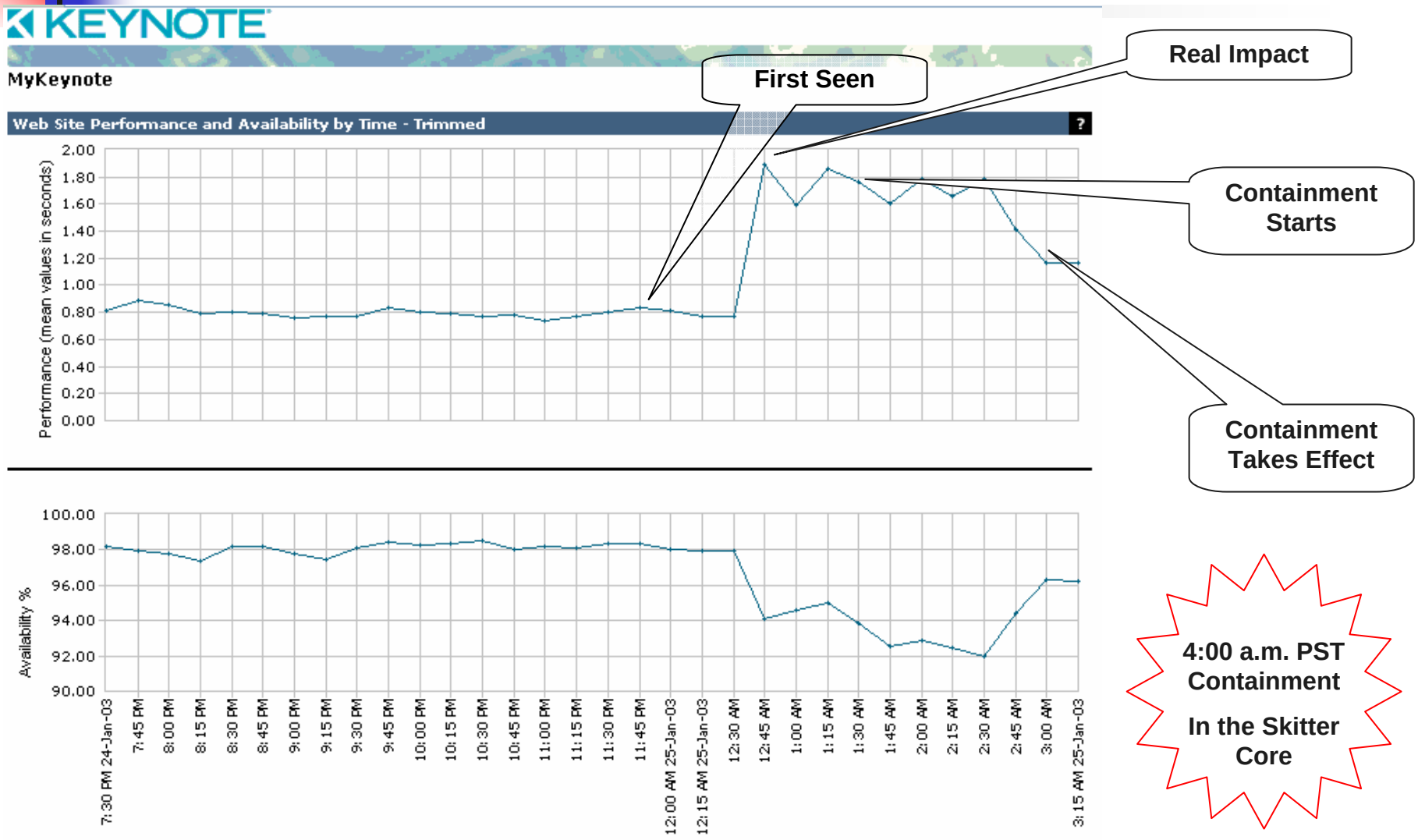
Decentralized Benefits - Blackout

- Aug 2003 North East/Canada Black Out knocked out power for the primary NSP-SEC computer right in the middle of proactive prep for the Blaster Worm.
  - Did it impact the Blaster preparation? No! People just E-mails and called each other (nsp-sec already got people in touch with each other)
  - Decentralized contacts allows for people to build their own “mitigation communities” when the centralize source gets knocked out.

NSP-SEC's Role during Slammer

- The SPs were the first to notice something was happening.
  - Circuits saturated, routers spiking, BGP sessions flapped, and customers complained.
- NSP-SEC was the first reporter of the worm. CERT/FIRST Teams got their alert from NSP-SEC.
- NSP-SEC members were the ones who captured the worm's packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm.

Impact of NSP-SEC's Containment



A few “Successes”

- eBay fraud team helping law enforcement arrest an average of 3.5 people per day world-wide
- Phishing sites last less than 5.5 days on average (some commercial protection firms claim 30 minute response)
- Several of the largest ISPs in the US are deploying subscriber notification and repeat offender escalation systems by 2008
- Changes to default configurations have reduced SMURF attacks, open SMTP relays (other attacks are now easier)
- Law enforcement in 50 countries have created a 24/7 assistance network for collection of electronic evidence (using or sharing the evidence after collection is still an problem)

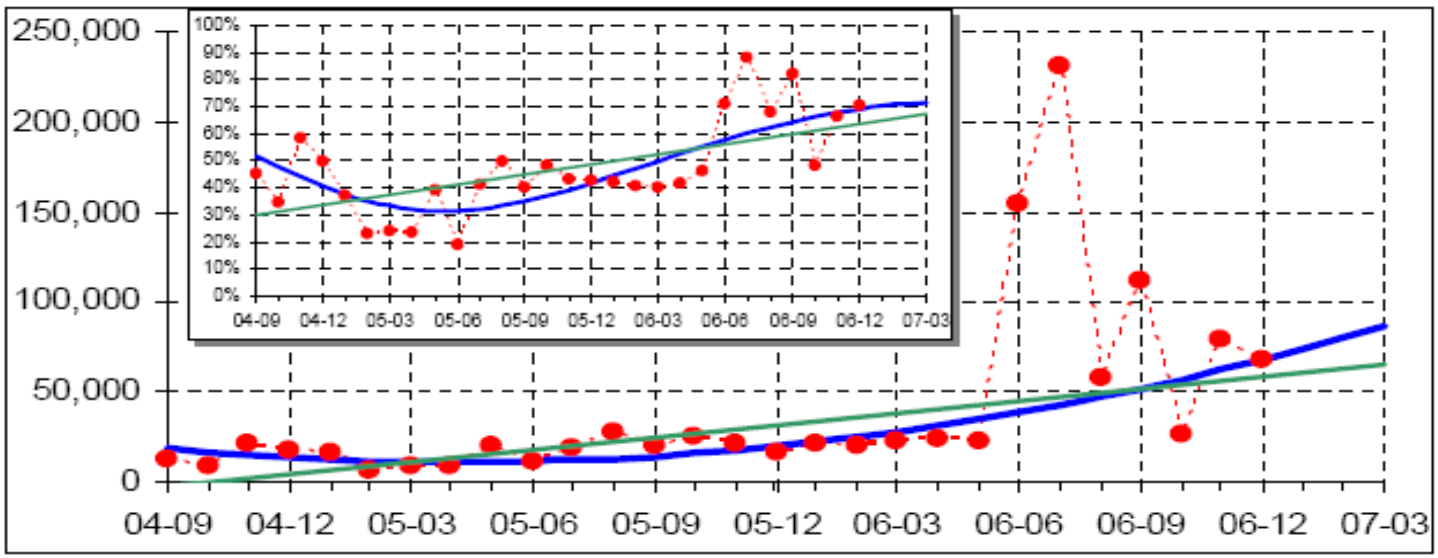
The scale of incident reporting

- A large ISP received (different years 2001-2006)
  - 4-6 million daily reports from public/subscribers
  - 1,000 criminal monthly requests
  - 30 civil monthly requests (90% legally defective)
- A large content owner (2006)
  - Made Over 1,000,000 DMCA complaints in 2006
- Spam reporting organization
  - Receives 11.6 submissions generates 21 complaints per minute
- Cyberbulling was reported to parents (50%), friends (33%), ISP (21%), teachers (6%) and LEA (1%)

Incident reports require analysis

9-1-1 Answering Points report 40%-60% of calls are not classified as emergencies after review

INHOPE – International Association of Internet Hotlines

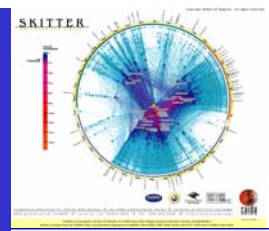


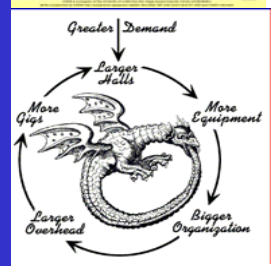
Number of Processed Reports about Other Content or Content which is Not Illegal
and as a percentage of the total reports processed..

Responding to incidents

- One ISP spent 15% of its monthly fees responding to abuse/security incidents
- Estimates range from 5 minutes to 4 weeks to remediate a compromised system
  - Users don't believe/don't read e-mail, old contact information, the Internet is more than just Web
  - Human assistance is limited by the number of knowledgeable people available
- Some victims don't want to believe they were victimized (and security products they use miss stuff)
  - Do the tools actually find all the problems
- If original cause is not addressed, repeatedly re-compromised
  - Technical cause, Social cause, Criminal cause

NSP-SEC Membership Requirement





NSP-SEC Membership Requirements

Membership in nsp-sec is restricted to those actively involved in mitigation of NSP Security incidents. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP Security incidents. That means no press and (hopefully) none of the "bad guys.“

http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC Membership Requirements

- Being a “Security Guru” does not qualify for NSP-SEC Membership.
- Being “from the *Government*” does not qualify for NSP-SEC Membership.
- You need to be someone who *touches* a router in a ISP/SP backbone, can tell someone to *touch* a router, offer some service to the forum, or develop BCPs for the community.
- NO LURKERS! If you do not contribute, you get punted off.

Application

- If you'd like to be considered for membership, please provide the following information via email to: nsp-security-owner@puck.nether.net

  Name:
  E-mail:
  DayPhone:
  24hrPhone:
  INOC-DBA Phone:
  Company/Employer:
  ASNs Responsible for:
  JobDesc:
  Internet security references (names & emails):
  PGP Key Location:

  For Job Description be as detailed and descriptive as possible. After sending the above form via email go to the section below and issue a "subscription" request via the form.

NSP-SEC

- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
  - Multiple Layers of sanity checking the applicability and trust levels of individuals.
  - Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC-AP

- NSP-SEC-AP – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
  - Multiple Layers of sanity checking the applicability and trust levels of individuals.
  - Not meant to be perfect – just better than what we had before.

- http://puck.nether.net/mailman/listinfo/nsp-security-AP

NSP-SEC-DISCUSS

- NSP-SEC is where the mitigation takes place. You do not learn anything, you are already expected to know.
- NSP-SEC-DISCUSS (NSP-SEC-D) is the place to learn, consult, work on new mitigation techniques, and lurk (if you want to).
- http://puck.nether.net/mailman/listinfo/nsp-security-discuss

NSP-SEC-D Membership

- People who would not qualify for NSP-SEC might qualify for NSP-SEC-D.
  - Vendors with Security Engineers developing products.
  - Security *Consultants* working with ISPs.
  - Security Researchers.
  - The masses of FIRSTs/CERTs

NSP-SEC-D Topics

- Best Common Practice (BCP) Development – working on new tools and techniques that will work in the community.
- Inter-Provider Coordination Procedures – learning from experience and moving forward.
- Proactive Forensic Analysis – Looking at what is going to happen, before it happens, and prepare proactive mitigation.

NSP-SEC Techniques & Tools

- Working with Empowerment Advocates to Teach the Community:
  - Remote Triggered Black Hole
  - Sink Holes configured as scan analyzers
  - Sink Holes configured as backscatter collectors.
  - BGP Prefix Filtering
  - ACLs

Mission Specific Groups

- NSP-SEC-LEO: Law Enforcement and Take Downs.
- Group of NSP-SEC members, law enforcement officers, and legal teams working on cyber-criminal take downs.

Regional Groups

- NSP-SEC-JP (Japan – In Japanese)
- NSP-SEC-BR (Brazil and other Portuguese speaking professionals)
- NSP-SEC-China (China – In Mandarin)

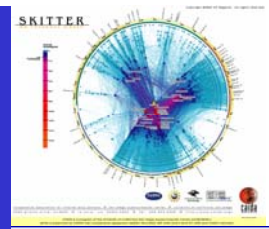
NSP SEC Meetings

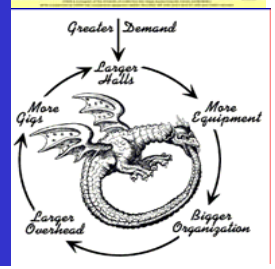
- NANOG Security BOFs (www.nanog.org)
- RIPE Security BOFs (www.ripe.net)
- APRICOT Security BOFs (www.apricot.net)
- SANOG Security BOFs (www.sanog.org)

What can you do to help?

- If you configure routers, are in operations, and handle ISP Security, then apply for nsp-sec membership:
  - http://puck.nether.net/mailman/listinfo/nsp-security
- NSP-SEC is looking for two or three engineers from each ISP who has the authority to configure routers and handle security incidents.

The Executive Summary





Where to go to get more?

- **NANOG Security Curriculum**
  - Sessions recorded over time which builds a library for all SPs to use for their individual training, staff empowerment, and industry improvements.
- http://www.nanog.org/ispsecurity.html

Top Ten List of things that Work

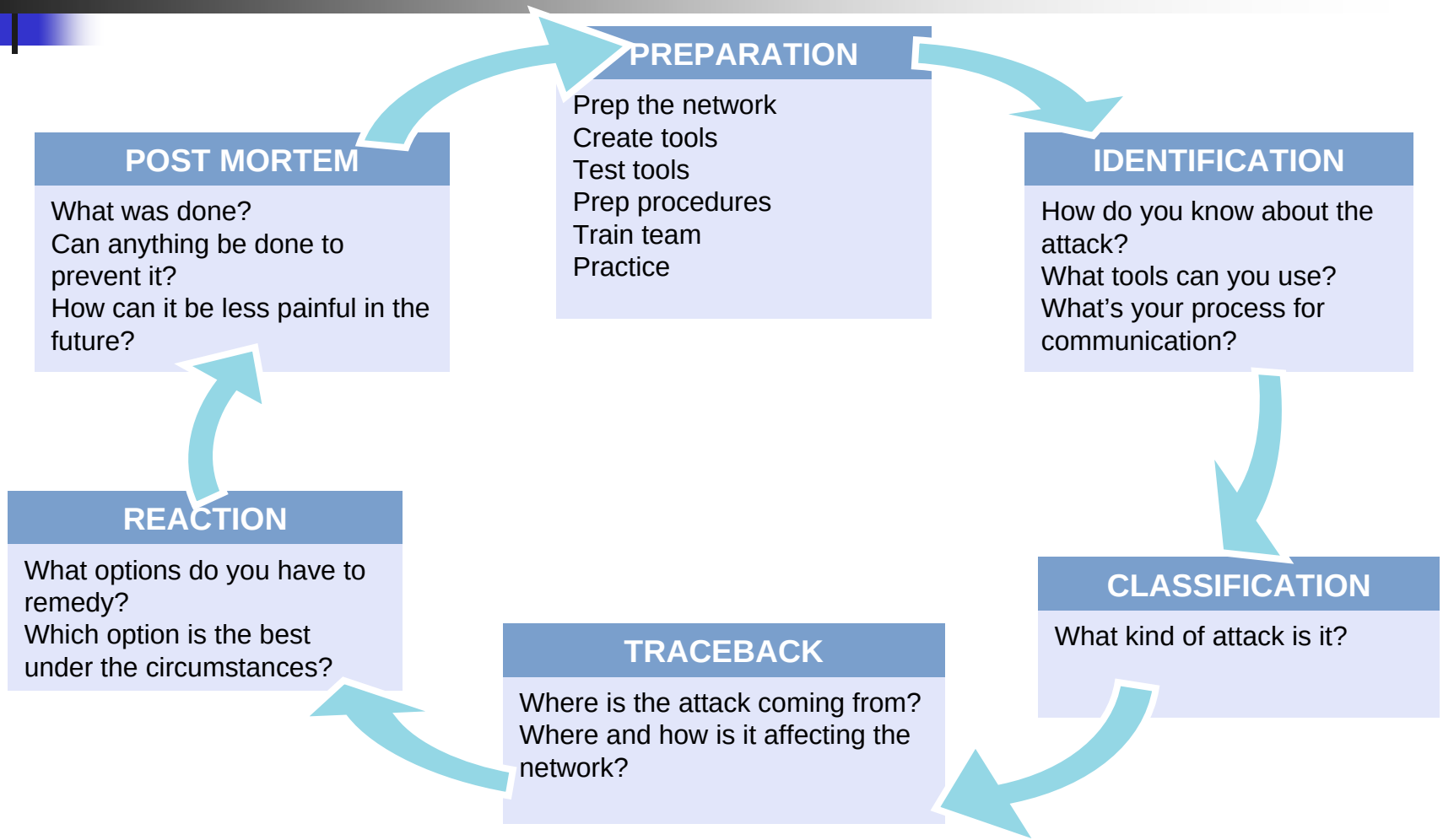
1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data Mining)

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

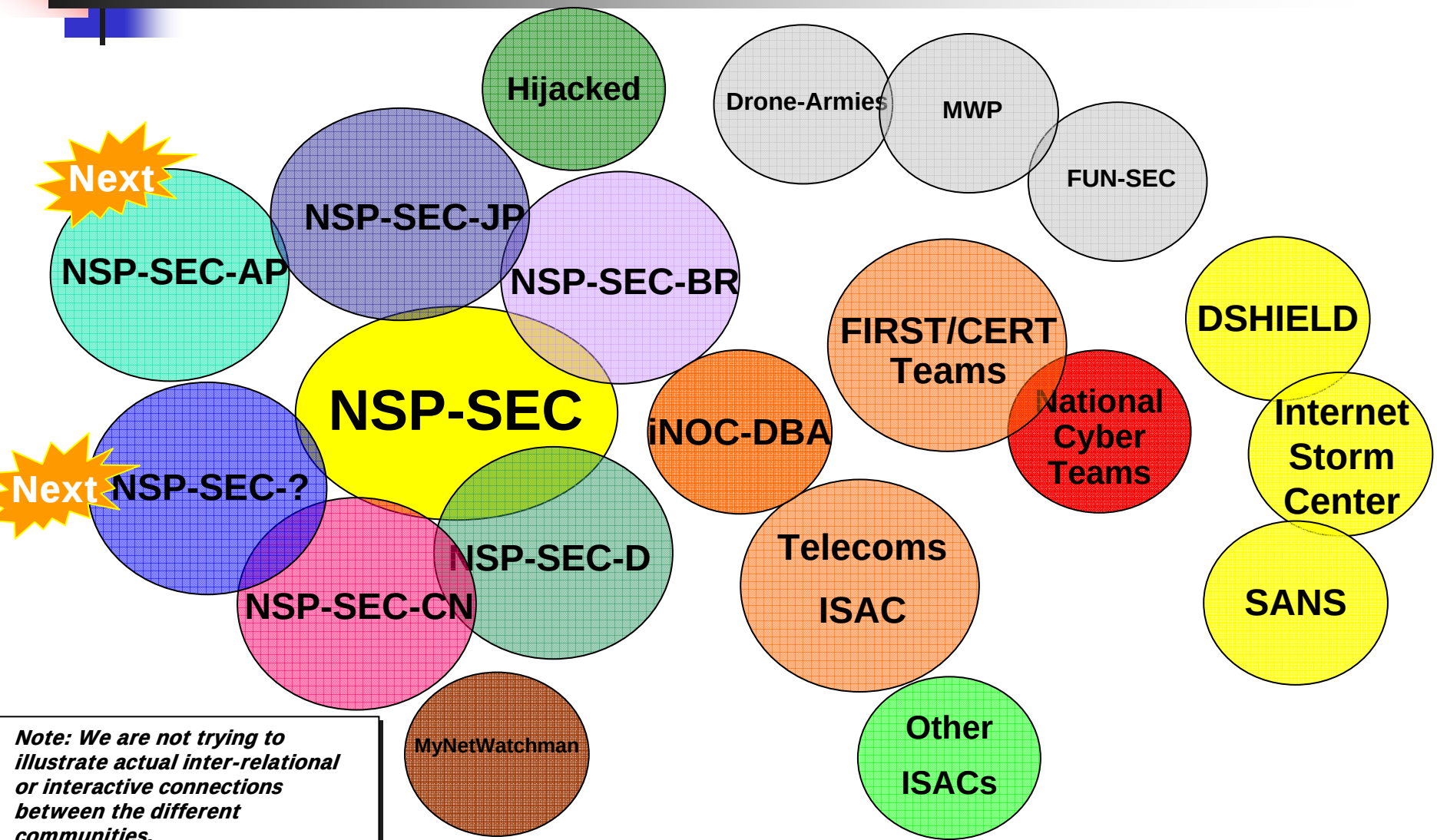
Sun Tzu

Art of War

SP Security in the NOC - Prepare



Aggressive Collaboration

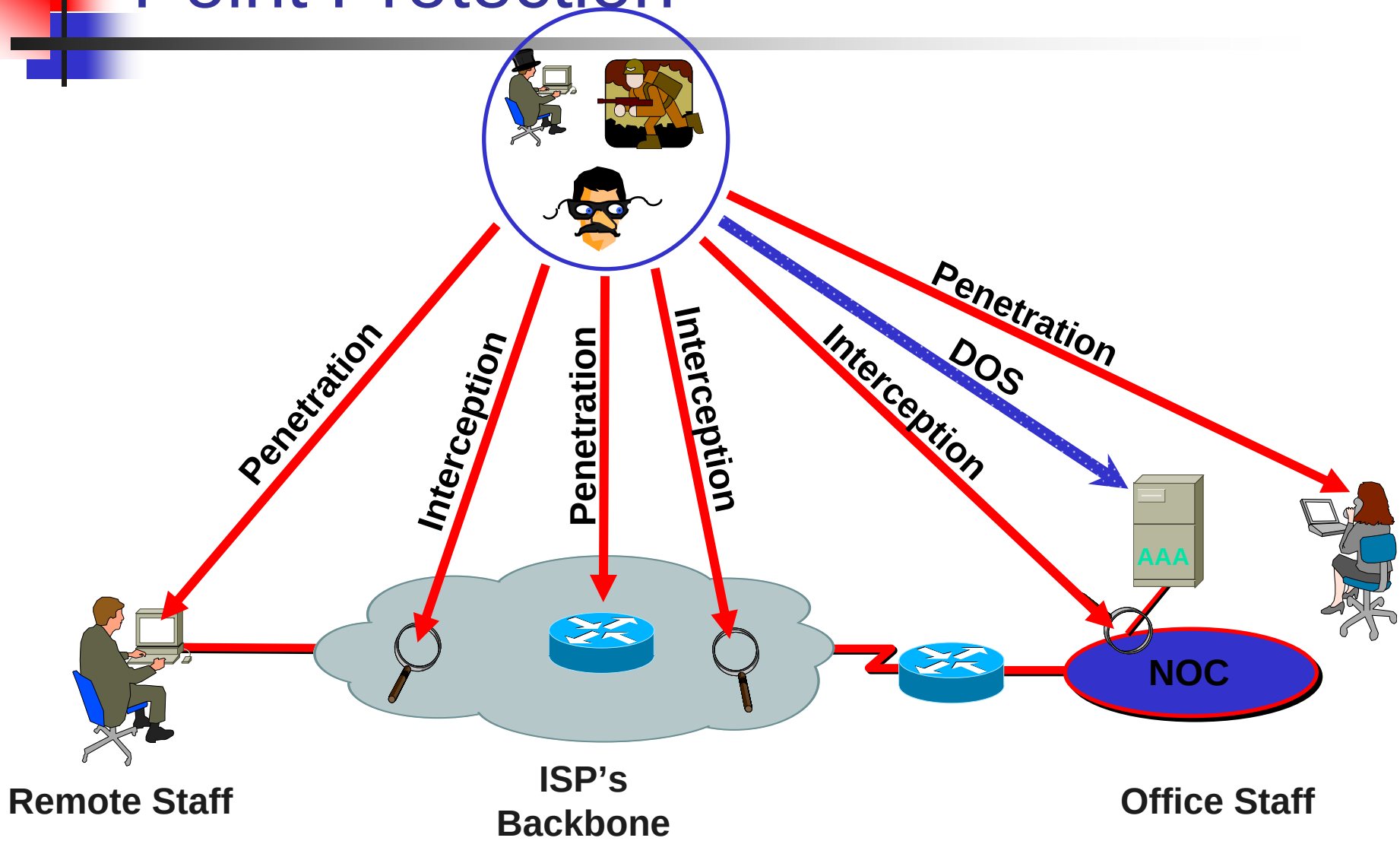


Note: We are not trying to illustrate actual inter-relational or interactive connections between the different communities.

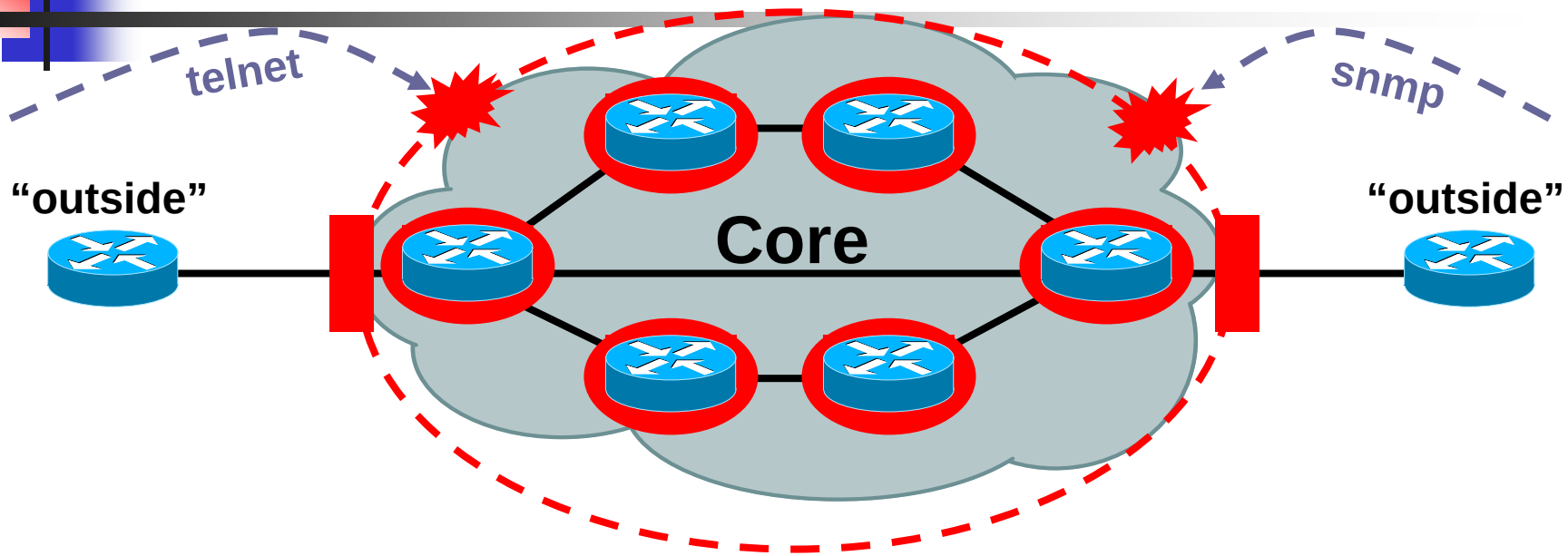
iNOC DBA Hotline

- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
  - ASnumber:phone
  - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net, and sponsored by Cisco.

Point Protection

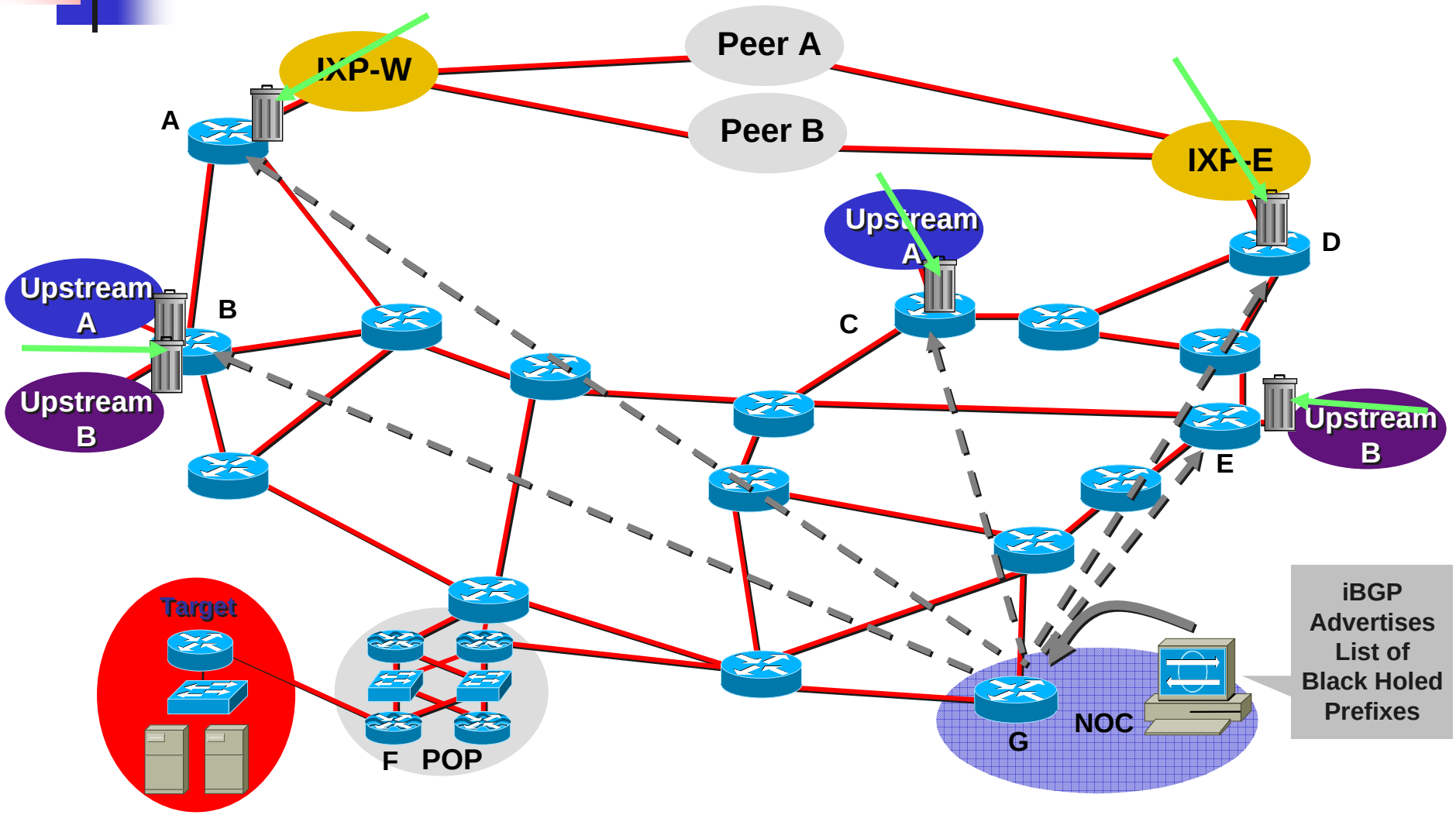


Edge Protection

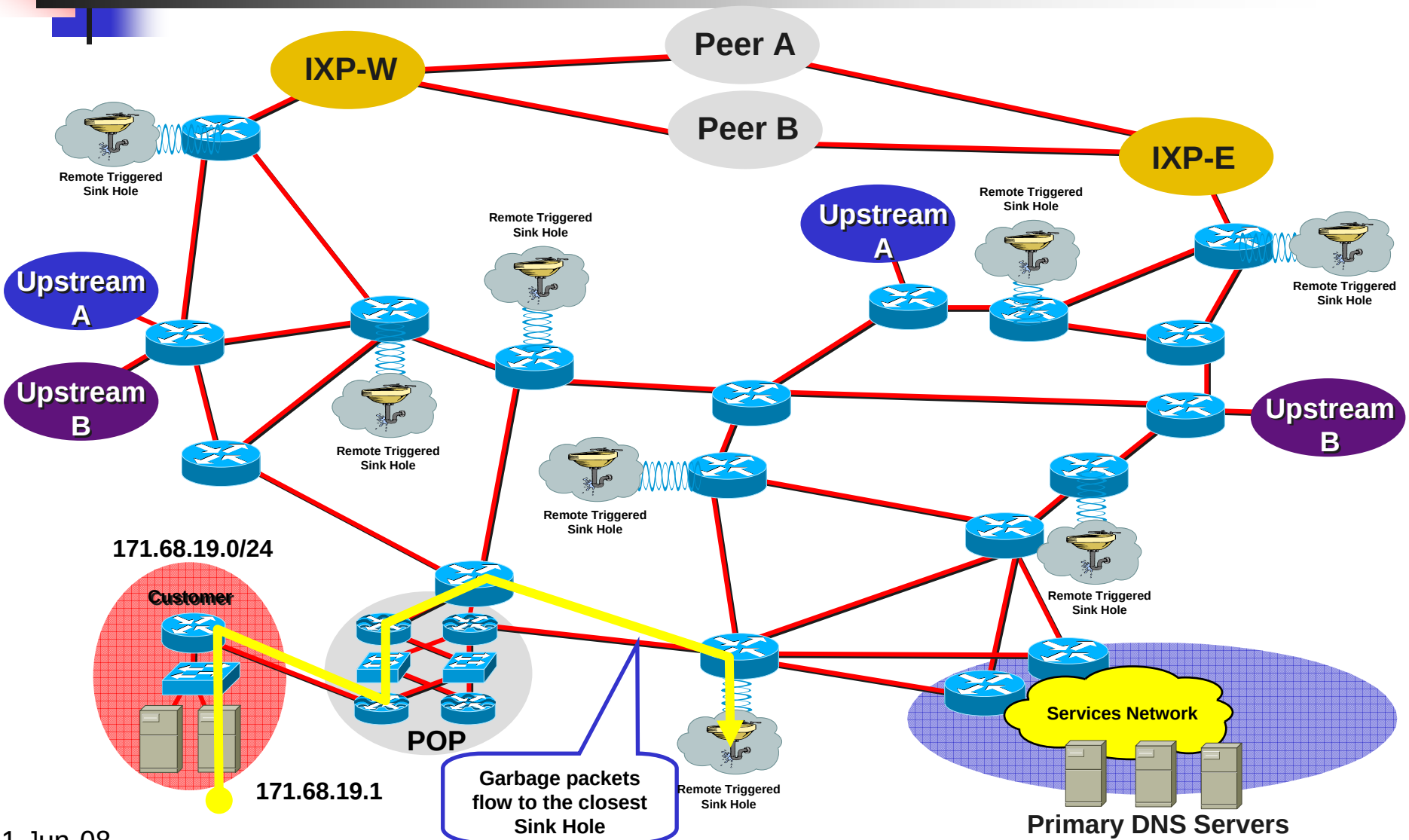


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH

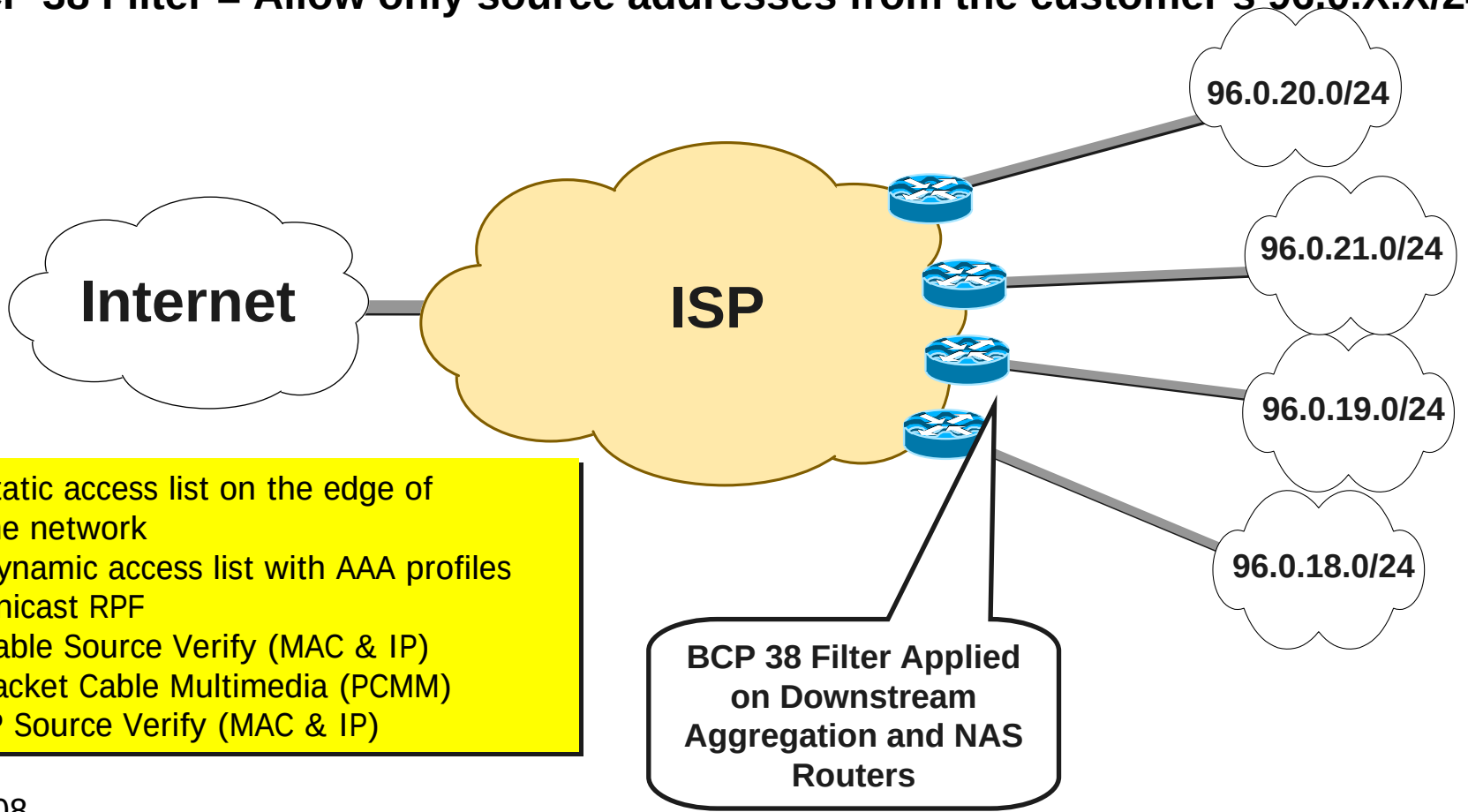


Sink Holes


IXP-W
Peer A
Peer B
IXP-E
Remote Triggered Sink Hole
Upstream A
Upstream B
Upstream A
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
171.68.19.0/24
Customer
POP
171.68.19.1
Garbage packets flow to the closest Sink Hole
Services Network
Primary DNS Servers

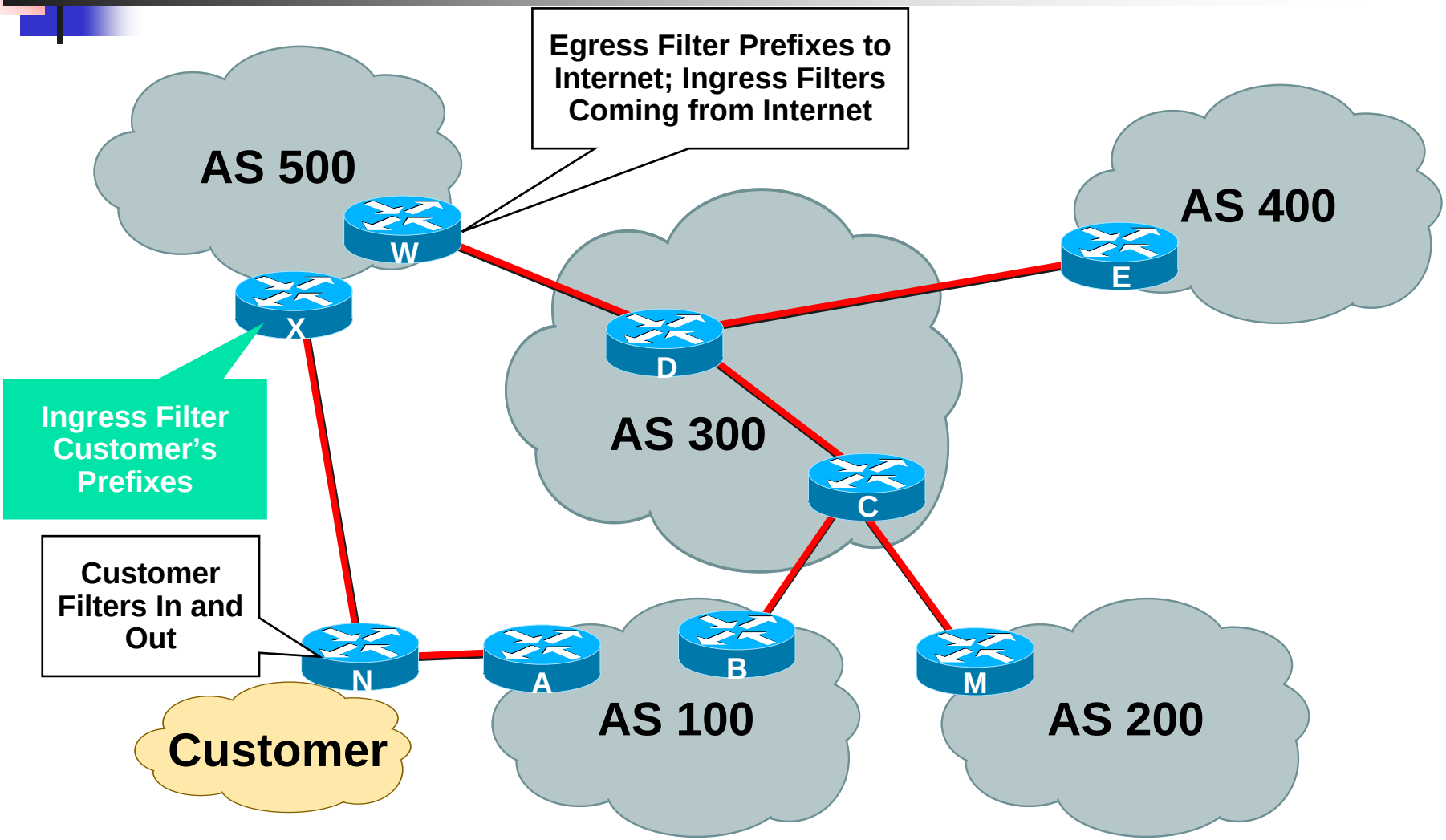
BCP 38 Ingress Packet Filtering

ISP's Customer Allocation Block: 96.0.0.0/19
BCP 38 Filter = Allow only source addresses from the customer's 96.0.X.X/24



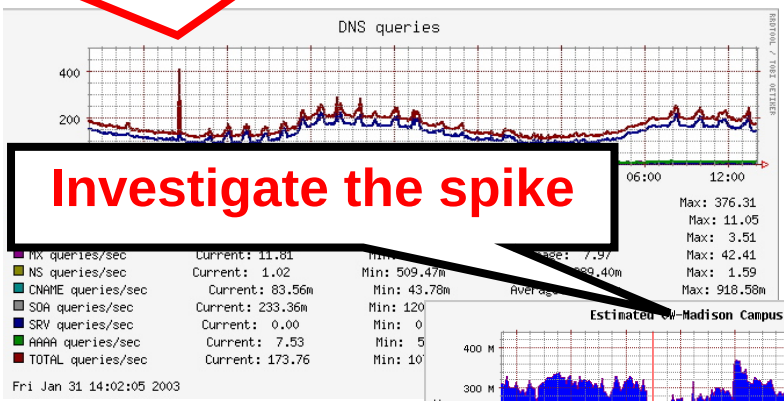
- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)

Where to Prefix Filter?

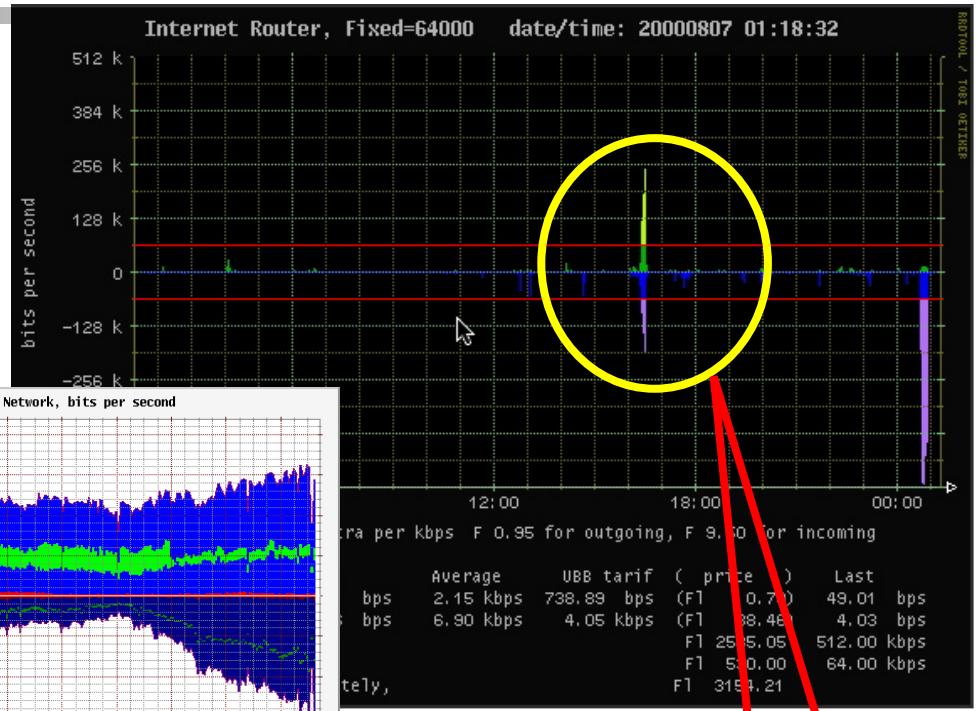


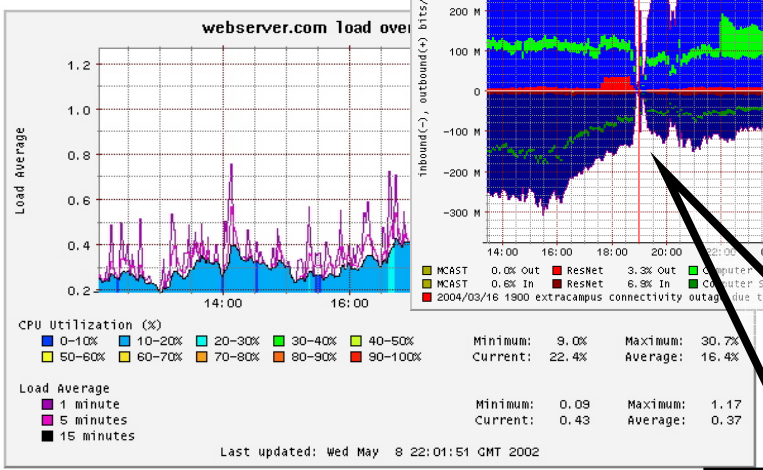
Total Visibility

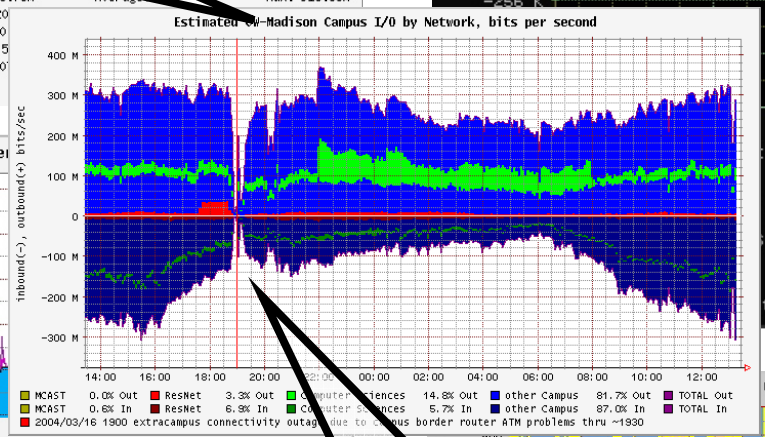
Anomaly for DNS Queries

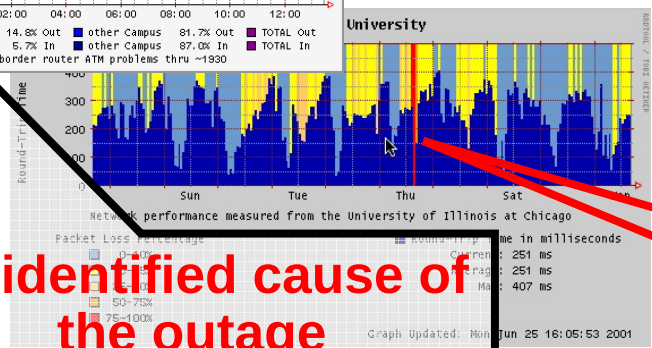


Investigate the spike









Thru'put Spike

RTT Spike

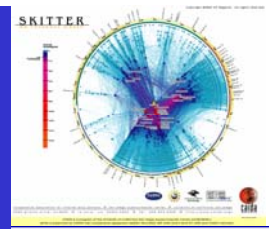
An identified cause of the outage

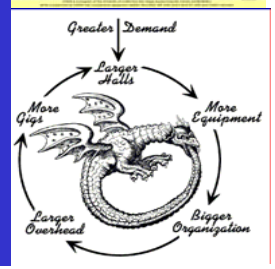
Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

What Really needs to be Done

- Consensus, Desire, but still in work
  - Core Hiding
  - Removed Coupled State Protection on Critical Infrastructure.
  - Architectural Approaches to Security
  - Re-Coloring (TOS/DSCP) at the Edge
  - Methodologies for effective SP oriented Risk Assessments.
- Working, but no Consensus
  - Common Services Ingress/Egress Port Blocking – (port 25, 53, 135, 139, 445)
  - DNS Poisoning

Communications Addendum





“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Preparation as Empowerment

- It is imperative that an SP's operations team prepare by empowering them for action.
  - Contacts for all ISPs who you inter-connect (peers, customers, and upstreams)
  - Contacts for all vendor's product security reaction teams.
  - Document your policies. Will you help your customers? Will you classify the attacks? Will you traceback the attacks? Will you drop the attacks on your infrastructure?

Important Points

- Create your company's Computer Emergency Response Team
- Know your peers (neighboring CERTs), build relationships
- Get on NSP-SEC mailing list and on iNOC Phone
- Know Each's Vendors Security Team

  Example: psirt@cisco.com, security-alert@cisco.com and www.cisco.com/security to contact Cisco Systems.

- Be prepared ! Define what to do & whom to contact for various incidents.

Step #1 – Take Care of Your Responsibilities

- Before knocking on doors to collect information on others, it is best that you take the time to insure you are fulfilling your responsibilities to facilitate communications.
- Make sure you have all the E-mail, phones, pagers, and web pages complete.
- Make sure you have procedures in place to answer and communicate.

OPSEC Communications

- Operations teams have a responsibility to communicate with
  - All peers, IXPs, and transit providers
  - Teams inside their organization
  - Customers connected to their network
  - Other ISPs in the community
- E-mail and Web pages are the most common forms of communication
- Pagers and hand phones are secondary communication tools

OPSEC Communications

Q. Does noc@someisp.net work?

Q. Does security@someisp.net work?

Q. Do you have an Operations and Security Web site with:

- Contact information
- Network policies (i.e. RFC 1998+++)
- Security policies and contact information

Q. Have you registered you NOC information at one of the NOC Coordination Pages?

- http://puck.nether.net/netops/nocs.cgi

SOC's Public Mailboxes

- RFC 2142 defines E-mail Aliases all ISPs should have for customer – ISP and ISP – ISP communication
- Operations addresses are intended to provide

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behavior
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries

/Security Web Page

- New Industry Practices insist that every IT company has a /security web page. This page would include:
  - Incident Response contacts for the company.
  - 7*24 contact information
  - Pointers to best common practices
  - Pointer to company's public security policies
  - Etc.
- See www.cisco.com/security as an example.

Emergency Customer Contact List

- E-mail alias and Web pages to communicate to your customer
  - Critical during an Internet wide incident
  - Can be pushed to sales to maintain the contact list
  - Operations should have 7*24 access to the customer contact list
  - Remember to exercise the contact list (looking for bounces)

Exercising the Customer Contact List

- Use Internet warning to look for bounces

Dear Customers,

You are receiving this email because you have subscribed to one or more services with Infoserve. We have received a virus alert from security authorities and we believe that you should be informed (please see information below). If you do not wish to be included in future information service, please click "Reply" and type "Remove from subscription" in the subject field.

We have received warning from security authorities on a new virus, W32.Sobig.E@mm. W32.Sobig.E@mm is a new variant of the W32.Sobig worm. It is a mass-mailing worm sends itself to all the email addresses, purporting to have been sent by Yahoo (support@yahoo.com) or obtained email address from the infected machine. The worm finds the addresses in the files with the following extensions: .wab .dbx .htm .html .eml .txt

You should regularly update your antivirus definition files to ensure that you are up-to-date with the latest protection.

For more information, please follow the following links:

Information from Computer Associates: http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=46275
Information from F-Secure: http://www.europe.f-secure.com/v-descs/sobig_e.shtml
Information from McAfee: http://vil.mcafee.com/dispVirus.asp?virus_k=100429
Information from Norman: http://www.norman.com/virus_info/w32_sobig_e_mm.shtml
Information from Sophos: http://www.norman.com/virus_info/w32_sobig_e_mm.shtml
Information from Symantec: http://www.symantec.com/avcenter/venc/data/w32.sobig.e@mm.html
Information from Trend Micro: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.E

Remember to Communicate

- Make sure there is someone behind all the E-mail aliases
- It is of no use to have a mean for people to communicate with your when you have no one behind the alias/phone/pager/web page to communicate back
- Many aliases are unmanned—with E-mail going into limbo

CERTs (Computer Emergency Response Teams)

- Origin: The Internet Worm, 1988
- Creation of “The” CERT-CC (co-ordination centre)
  - Carnegie Mellon University, Pittsburgh http://www.cert.org/
- The names vary:
  - IRT (Incident Response Team)
  - CSIRT (Computer security incident response team)
  - ... and various other acronyms
- Start with the following URLs:
  - www.cert.org
  - www.first.org

How to Work with CERTs

- Confidentiality
- Use signed and encrypted communication

  Use PGP, S/MIME or GPG, have your key signed!
- CERTs coordinate with other CERTs and ISPs
- CERTs provide assistance, help, advice
- They do not do your work!

BRG1 Recommended

Any SP who isung IP as business should invest. It is essentials.

Sales tool.

Barry Raveendran Greene, 11/17/2005

Collecting Information from Peers

- Do you have the following information for every peer and transit provider you interconnect with?
  - E-mail to NOC, abuse, and security teams
  - Work phone numbers to NOC, abuse, and security teams
  - Cell Phone numbers to key members of the NOC, abuse, and security teams
  - URLs to NOC, abuse, and security team pages
  - All the RFC 1998+++ remote-triggered communities

Questions

Q. Do you have the NOC and Security Contacts for every ISP you are peered?

Q. Do you test the contact information every month (E-mail, Phone, Pager)?

Q. Have you agreed on the format for the information you will exchange?

Q. Do you have a customer security policy so your customers know what to expect from your Security Team?

Over Dependence on Vendors–Danger!

- Operators who use their Vendors as Tier 2 and higher support endanger their network to security risk.
  - Vendors are partners with an operator. They should not maintain and troubleshoot the entire network.
  - Way too many operators today see a problem on a router and then call the vendor to fix it.
  - This is not working with Turbo Worms.

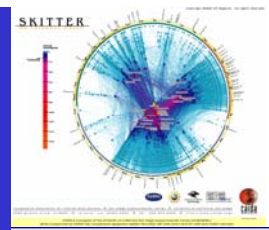
Hardware Vendor's Responsibilities

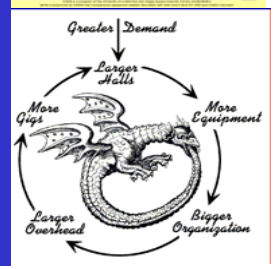
The roll of the hardware vendor is to support the network's objectives. Hence, there is a very synergistic relationship between the SP and the hardware vendor to insure the network is resistant to security compromises

What you should expect from your vendor?

- Expect 7x24 Tech Support (paid service)
- You should not expect your vendor to run your network.
- Membership in FIRST (http://www.first.org/about/organization/teams/)

Other Groups





CERT & FIRST

- Find a CERT/FIRST Team to work with.
  - Important avenue of community communication - Forum of Incident Response and Security Teams
  - Consider becoming a FIRST Member.
  - Protect yourself - SP RFPs need to require FIRST/CERT Membership.

http://www.first.org/about/organization/teams/

Information Sharing and Analysis Centers (ISACs)

- Vital part of Critical Infrastructure Protection (CIP)
- Gather, analyze, and disseminate information on security threats, vulnerabili incidents, countermeasures and best practices
- Early and trusted advance notification of member threats and attacks
- Organized by industry: cross-sector awareness, outreach, response and recovery