Attack Fingerprint Sharing: The Need for Automation of Inter-Domain Information Sharing

RIPE 50

Stockholm, Sweden

Danny McPherson danny@arbor.net

May 3, 2005

Agenda

- What’s a “bot” and what’s it used for?
- Evolution of threats & problem scope
- Attack Traceback and Mitigation
- Inter-domain sharing of attack information
- Fingerprint Sharing
- Summary

- *Disclaimer: I was asked to talk about Arbor’s “Fingerprint Sharing Alliance” - attempted to keep this as non-commercial as possible*

What’s a “bot”?

- A ***bot*** is a servant process on a compromised system
- Usually installed by a ***trojan***, though worms have evolved to install bots as well (e.g., deloder)
- Communicates with a handler or controller, typically via IRC, often running on public IRC servers or other compromised systems
- Almost always unbeknownst to the systems owner - ‘got bot?’
- A ***botmaster*** or ***botherder*** commands bots to perform any of an number of different functions
- System of bots and controller(s) is referred to as a ***botnet*** or ***zombie network***

Escalation of Worm Threat

- Escalation of threat in worm payload
- Clear trend from worms that simply wreak havoc and disrupt network services to worms that enable bot proliferation
- An entire miscreant economy exists - don’t want to violate SLAs with worm-triggered network services disruption

Escalation of Threats..

- For example:
  - Code Red: DDoS against one IP
    - Changed IP/Null routed previous IP
  - Blaster: DDoS against hostname
    - Repeated DNS Shifts
    - Eventual NXDOMAINing of windowsupdate.com record
  - Deloder: Arbitrary DDoS toolkit
    - Hrmm…?
- Backdoors escalated from remote control (e.g., BO, NetBus) to harvesters and far more complicated
  - NetBus was originally written in March of 1998 and only had Swedish UI. In November of 1998 it was translated to English and it's use continues to grow even today!
- Control channels include IRC commonly and other, encrypted mechanisms more and more.

What’s a botnet used for?

- Bots are used for one **or more** of the following:
  - Install key loggers and capture passwords, account information, etc../ ID Theft
  - Gain access to local LANs or internal systems
  - Phishing
  - Spam relay/harvest email addresses for spammers
  - Open proxies
  - DOS Attacks
  - Distributed cracking systems (e.g., Brute Force SSH activity)
  - New Rbot capabilities include using webcams to capture video and still images(!)
- An entire economy is evolving around bot ownership
  - Sell and trade of bots ($0.10 for “generic bot”, $40 USD or more for an “interesting” bot; e.g., a .mil bot)
  - Bots are a commodity - no significant resource constraints

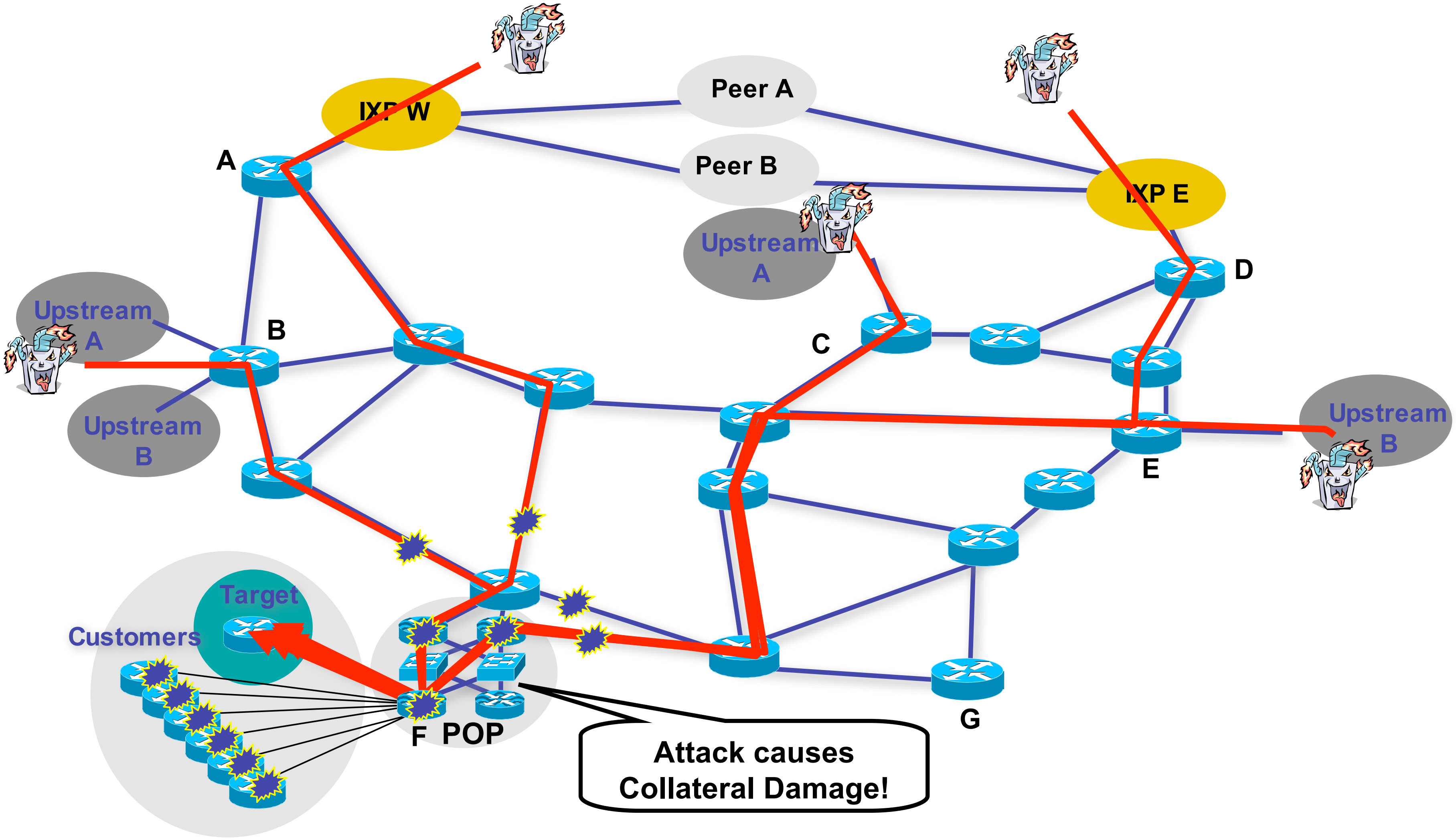
How big is the problem?

- As many as 157,000 new bots recruited every day according to a recent report by CipherTrust!
- Symantec’s latest Internet Security Threat Report reports that bot observations currently average 30,000 a day
- A single botnet comprised of more than 140,000 hosts was observed “in the wild” over 3 years ago
- Botnet driven attacks have been responsible for single DDOS attack flows of more than 10Gbps aggregate capacity
- A study conducted by the University of Michigan showed that an out of the box Windows 2000 PC was recruited into 3 discrete botnets upon being connected to the Internet for just 48 hours - Numerous studies reinforce similar infection rates/frequencies

I’m responsible for the infrastructure - why do I care?

- Many of the compromised hosts reside on your internal network or belong to customers of yours - it’s your responsibility…
- And if that doesn’t work?
  - The sheer size of these botnets and available firepower not only thoroughly neutralize the target, they also yield a considerable amount of collateral damage on the infrastructure - your network!
  - Consider the fact that an OC-3 (155 Mbps) could be effectively rendered useless by a botnet comprised of only 200 home PCs, each with an average connection bandwidth of only 1 Mbps
  - Now, consider frequency of recruitment and couple that with proliferation of residential broadband access capacities - are you concerned yet?
  - …and couple that with the evolving convergence architectures in IP networks today (e.g., VoIP, Video, Internet, VPN) and overlay services availability requirements --
- Now do you care?

Collateral Damage

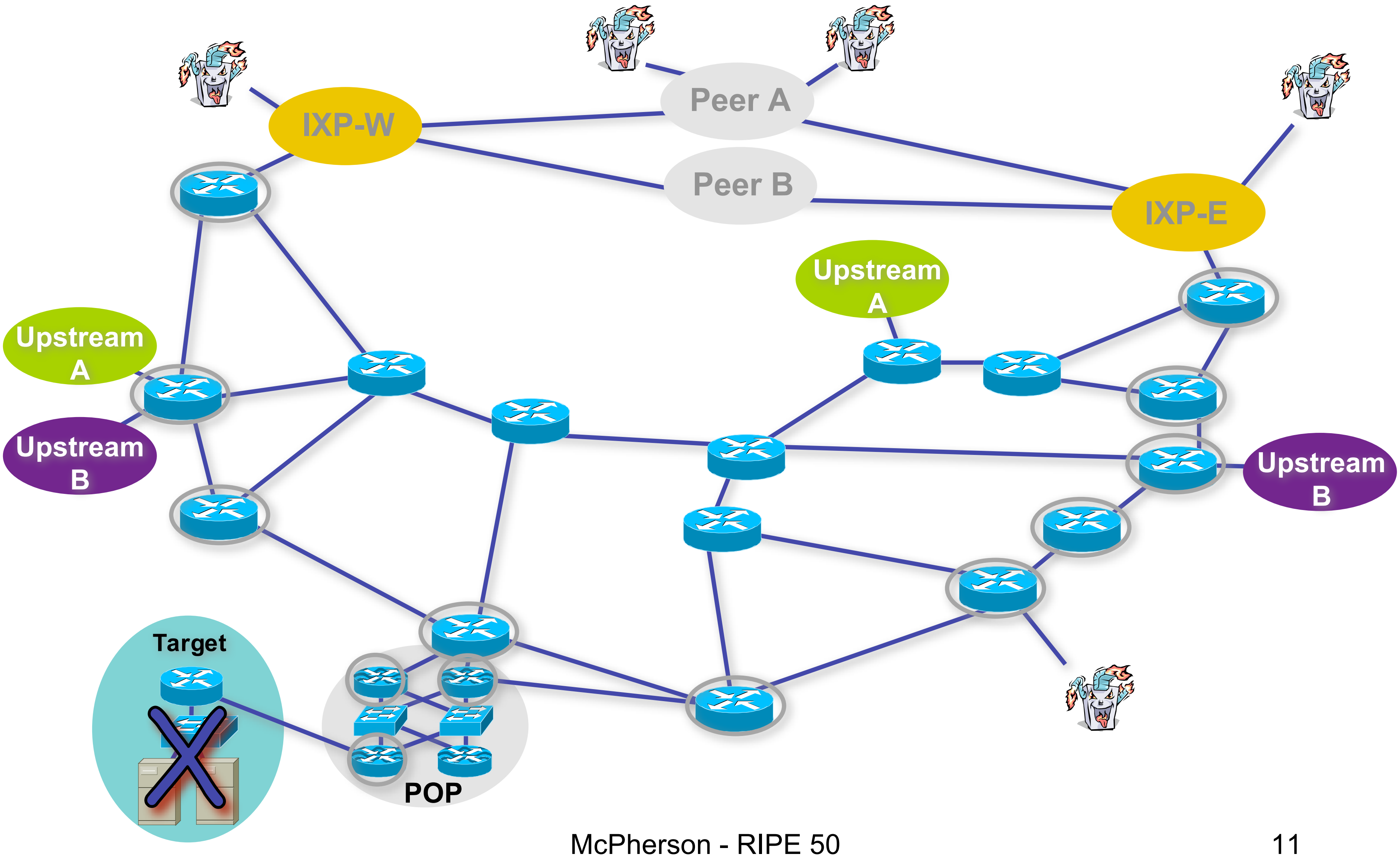


Attack causes Collateral Damage!

Traditional Traceback & Mitigation

- Began with ACLs and counters at network egress to customer
- Filtered attack traffic as it was destined for customer premise
- Manually traced back through the network, hop-by-hop, interface by interface - very time-consuming and tedious (automated with ACL scripting tools; I.e., dostracker.pl)
- Then BGP Blackholing…
- Backscatter Traceback, employing BGP blackholing techniques (may not identify ingress interface - assumes spoofing)
- However, attack magnitudes grow, inflict collateral damage on aggregation routers and inter-POP/intra-POP links, and therefore must be mitigated at network ingress

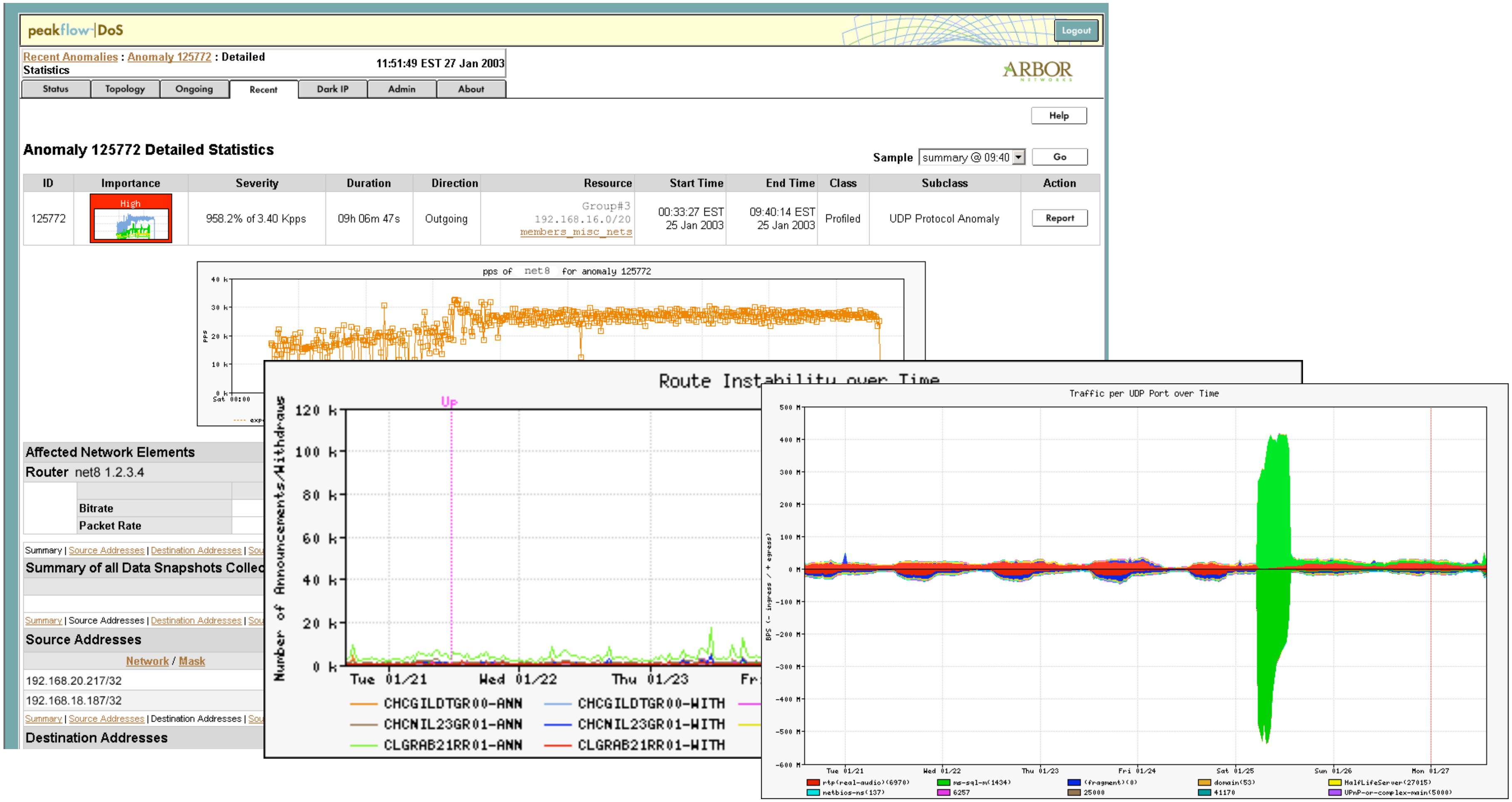
Traditional Traceback



Optimized Traceback

- Flow-based detection tools (open & commercial) and traceback, covering entire network perimeter, real-time alerting (as opposed to a customer calling?), augments infrastructure
- NetFlow and sFlow-based techniques, IPFIX perhaps in the future… to report on Network and Transport attributes of an attack, as well as any other interesting micro-flow characteristics
- Flow-based techniques enable mitigation that’s element specific, sequentially optimized, performed at network ingress, with full accounting (even BGP Blackhole packets and the like), forensics, etc..

Optimized Traceback



peakflow | DoS

Recent Anomalies : Anomaly 125772 : Detailed Statistics   11:51:49 EST 27 Jan 2003

Status | Topology | Ongoing | Recent | Dark IP | Admin | About

Anomaly 125772 Detailed Statistics

Sample: summary @ 09:40 Go

ID	Importance	Severity	Duration	Direction	Resource	Start Time	End Time	Class	Subclass	Action
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing	Group#3 192.168.16.0/20 members_misc_nets	00:33:27 EST 25 Jan 2003	09:40:14 EST 25 Jan 2003	Profiled	UDP Protocol Anomaly	Report

Affected Network Elements

Router net8 1.2.3.4

	Bitrate
	Packet Rate

Summary | Source Addresses | Destination Addresses | Sou

Summary of all Data Snapshots Collec

Summary | Source Addresses | Destination Addresses | Sou

Source Addresses

Network / Mask
192.168.20.217/32
192.168.18.187/32

Summary | Source Addresses | Destination Addresses | Sou

Destination Addresses

And that’s still not good enough!

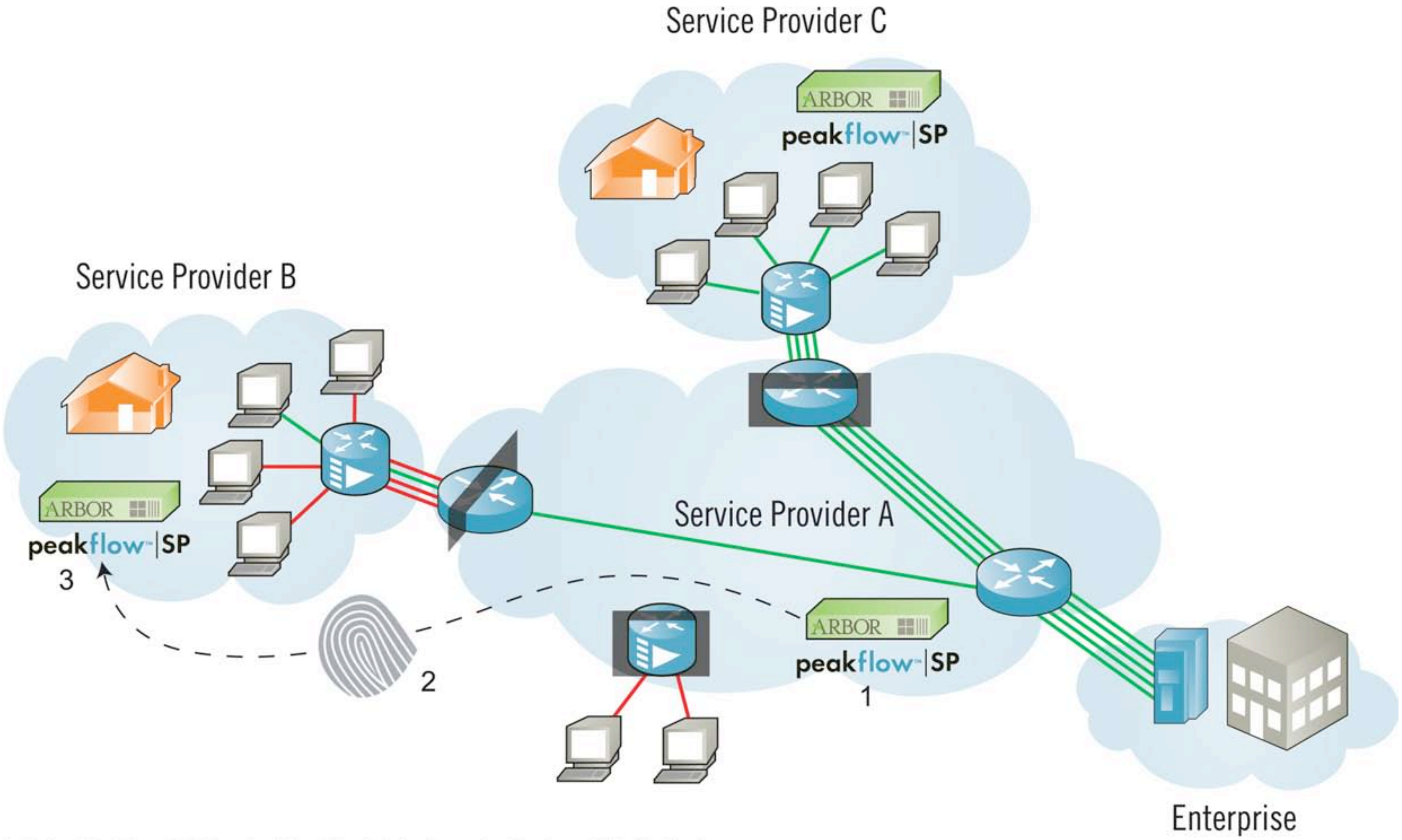
- Mitigation must occur as farther upstream, else network interconnect bandwidth is affected
- In order to effectively eliminate threats identities (and associated attributes) of compromised hosts must be conveyed to “Internet” ingress network - or as close to source as possible
- With infection/compromise frequency and available firepower, botnet information must be shared in an automated manner - quarantine and remediation functions MUST be automated as well!

Sharing Requirements

- Attack sources and attributes can only be shared with transit and origin networks (don’t share information with “third parties”
  - Couple routing information to determine source and transit networks
- Must be shared via secure mechanism
- Employ a common language for describing attacks
- Must be trackable
- Must provide peer-peer registration process
- Must employ distributed architecture with peer-peer and centralized fingerprint distribution model
- Can be used for sharing explicit attack attributes, as well as worm and vulnerability signature information
- Information can be shared with adjacent and non-adjacent networks
- Needs to interface with non-Arbor systems
- Needs to be multi-vendor

Fingerprint Sharing Alliance

FINGERPRINT SHARING: HOW IT WORKS



1. Using Peakflow SP, Service Provider A detects and mitigates a DDoS attack.
2. Service Provider A securely sends the attack “fingerprint” to the relevant upstream providers affected by the attack.
3. After securely receiving the fingerprint, the information is used by the upstream ISP to traceback, analyze, and mitigate the attack, thereby identifying and removing compromised hosts as close to the internet ingress points as possible.

Other Attack Information Conveyance Mechanisms

- Peer-Peer
- INOC-DBA
  - http://www.pch.net/inoc-dba
- NSP-SEC
  - https://puck.nether.net/mailman/listinfo/nsp-security
  - https://puck.nether.net/mailman/listinfo/nsp-security-discuss
- IETF INCH/RID
  - http://www.ietf.org/html.charters/inch-charter.html
- BGP Flow Specification?
- Other?
- Arbor Networks
  - http://www.arbor.net

Summary & Conclusions

- Providers MUST work together to solve this problem
- Bot detection AND response mechanisms MUST be automated
- Protection and cleaning of the host is where the problem should be resolved -- in the interim network operators will inevitably be required to intervene - if not to protect their customers, at least to protect themselves
- Attack fingerprint sharing and similar mechanisms need to be further researched, developed and deployed to combat this very real threat

Thanks!

danny@arbor.net