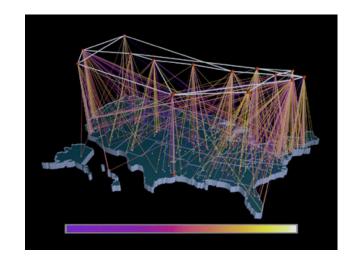
Internet Traffic Trends A View from 67 ISPs

Craig Labovitz (labovit@arbor.net)

Danny McPherson (danny@arbor.net) Scott lekel-Johnson (scottij@arbor.net) Mike Hollyman (mhollyman@arbor.net)

Internet Statistics

- Golden Age
 - NSFNet 1986-1995
 - Monthly ARTs reports
 - protocol, ports
 - Filtered prefix reports



- Today
 - Some ISP specific traffic research and commercial datasets
 - e.g. Akamai, Google, etc.
 - Lots of BGP data
 - Many, many analyst reports
 - Mostly people make stuff up

Internet Traffic Project

Global view of Internet traffic and attack trends

- Leverage commercial probe deployments
 - Pool of 2,500+ active Flow / DPI collectors
 - Across 250 ISPs / Content Provider / Higher Ed
 - Deployed adjacent interesting bits of infrastructure
- Internet scale data collection
 - Traffic, DPI, Mitigation and Security datasets
 - Geographically and topologically diverse

Internet Traffic Project

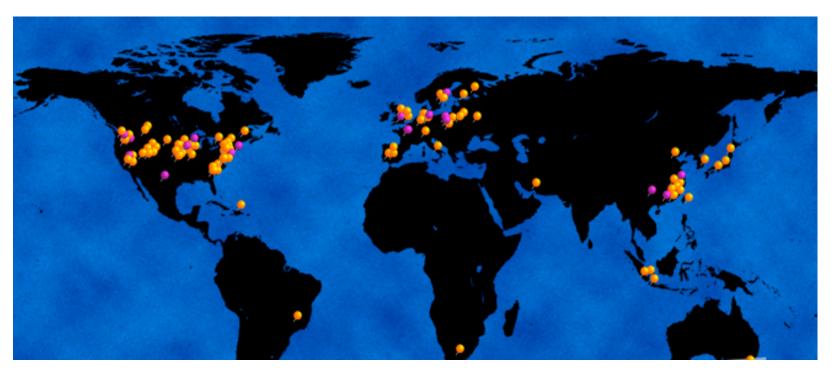
Outgrowth Fingerprint Sharing
 Initiative

THE WALL STREET JOURNAL. Firms Join Forces Against Hackers

BY RIVA RICHMOND DOW JONES NEWSWIRES

- 45 publicly disclosed participants
- and Annual ISP Security Survey
- All data voluntary anonymous data sharing agreement with ISPs
- Still more research project than commercial
 - Arbor, University of Michigan, Princeton (Intern)
 - And 78 ISPs (and growing)

Internet Traffic Deployment



- 67 long-term participants (2 years)
- 17 unique countries
- 27 in US, though many have global footprint

Current Traffic Project Deployment

- 67 long-term ISPs (now 78)
 - 5 MSO, 4 Tier1, 15 Tier2, 4 Content, 1 R&E
 - Remainder not self-catagorized
- 1,270 routers
- 141,629 interfaces
- > 1.8 Tbps of average inter-domain traffic
- 485 days and counting (began September 2006)

Typical ISP Deployment

- Majority deployments are Flow from all peering edge routers
 - NetFlow / JFlow/ Sflow / IPFIX / etc
- Growing DPI from gigabit inline / portspan in front of customers or server clouds
- Exported to commercial probes
 - Usually 1/100 1/000 sampling
 - Regexp or BGP based classification of border interfaces to avoid double counting
 - Data validated against interface SNMP counters

Anonymous XML Data

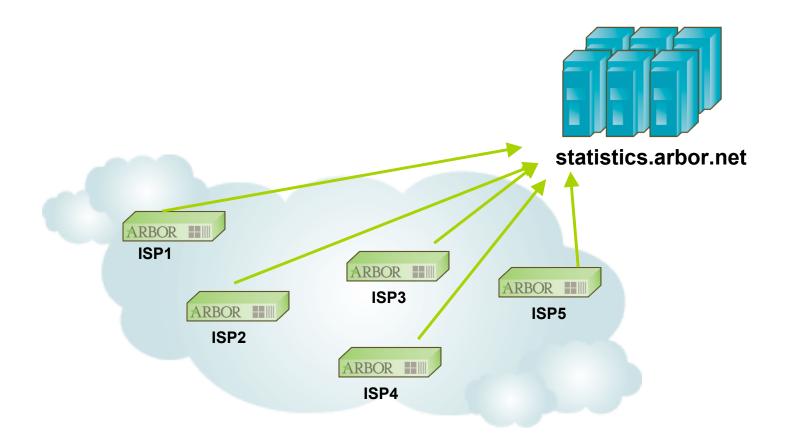
- Five minute traffic samples
 - Traffic In/out of network (subset of backbone traffic)
 - Cross-products based on top N protocols, ASNs, ports, applications, etc.
- Traffic anomaly data
 - Combination protocol signatures, behavior and statistical variance from baselines
 - Distinguish Attack versus Flash Crowd
 - Annotations and mitigation status
- Self-Categorization
 - Tier1/2/3, Content, High Ed, etc
 - Predominant geographic coverage area

```
- carbor_stats version="4.0" device= 'CP' sp_version="4.
   <time>1212422716</time>
 + <description></description>
 + <legal_text> </legal_text>
 + <info devices='5" routers='24' interfaces='1431" ma
 - <attack id="158297" start="2008-05-02-00:47:25" stop</p>
     <severity importance="2" lrm="1478.525" red_rati
     -dimpact bps="0" pps="0"/>
     <type cluss="1" subcluss="3"/>
     -cdirection type="Outgoing" name="anonymous" gie
     coretocols>6</pretocols></pretocols>
     <tcpflags>SAFP</tcpflags>
   - COURCES
       <ips>xx.xx.161.114/32>
       orts-41433-/ports-
     </sectors/
   - olsta
       <ipc>136.1.1.253/32</ipc>
       <ports>8000</ports>
     cidate
     <infrastructure num_routers='1" num_interfaces:
   </attack>
- sattack id="158296" start="2008-05-02-00;47:25" stop
     <severity importance="1" Irm="1475.776" red_rati
     dmpact bps="0" pps="0"/>
     <type class="1" subclass="2"/>
     «direction type="Outgoing" name="anonymous" git
     cpretocols>6</pretocols>
     <tepflags>SAFP</tepflags>
   - CODUCCED
       <ip><ip>xx.xx.161.114/32</ip>>
       <ports>41433</ports>
     <3081062>

   - olst>

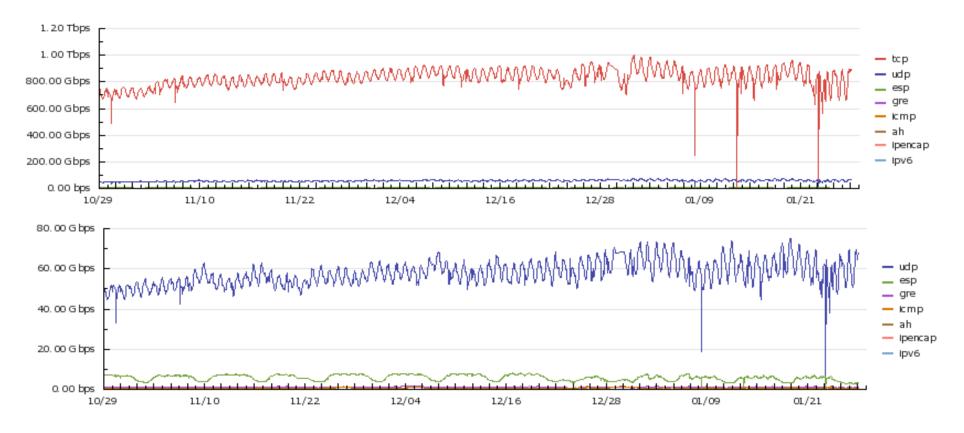
       <lps>136.1.1.253/32</lps>
       <perts>8000</perts>
     <idst>
     <infrastructure num_routers='1" num_interfaces=
   </attack>
 - - cattack id="158298" start="2008-05-02 00:52:32" stop
```

Internet Traffic Project



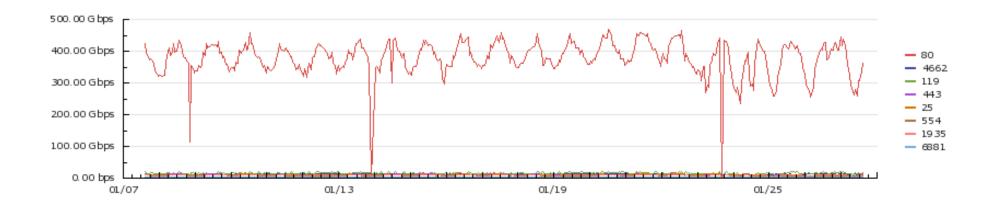
- Each participating ISP deployment submits XML
- Anonymous XML over SSL every hour
- Arbor managed servers collect/process

90 Day Protocol Distribution Trends



- No real surprises: TCP dominates followed by UDP
- Possible North America / Europe bias to dataset given diurnal patterns
- Wither IPv6?

60 Day TCP Port Trends

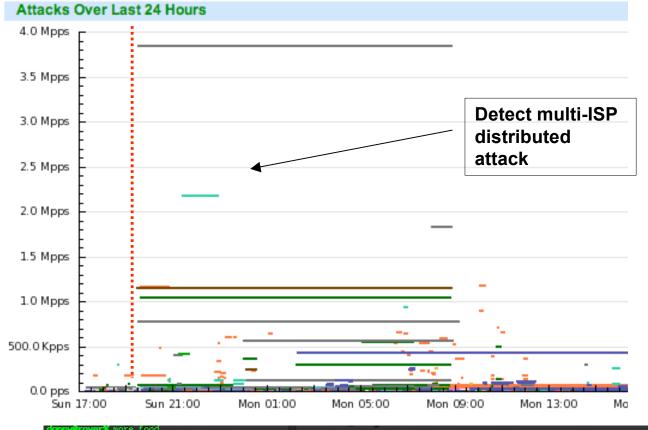


- Again, no surprises: http/80 by far most prominent TCP port
- In second place, TCP/4662 (edonkey) most prominent inter-domain peer-2-peer file sharing protocol
- Rises of NNTP (ranks 3rd) as file sharing alternative (alt.binaries!)

Internet Anomaly / Attack Summary

- 485 days
- Anomalies
 - 616,631 total anomalies reported
 - 1,271 average anomalies/day
- Attacks
 - 353,588 classified attacks (57.34%)
 - 729 average attacks/day

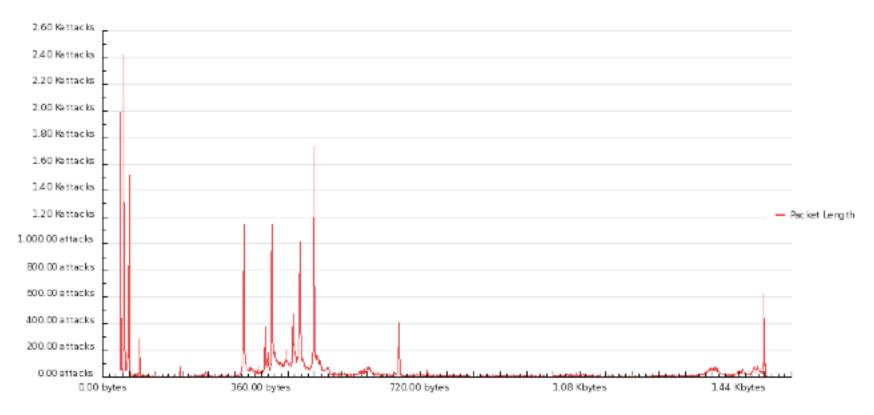
Internet Attack Propagation



- Each color represents different anonymous ISP (30 represented)
- Each line represents different attack
- 7 Outbound ISPs, 10 attack streams (7 tcpsyn, 3 icmp) generating 6.312 Mpps, one Russian AV Vendor

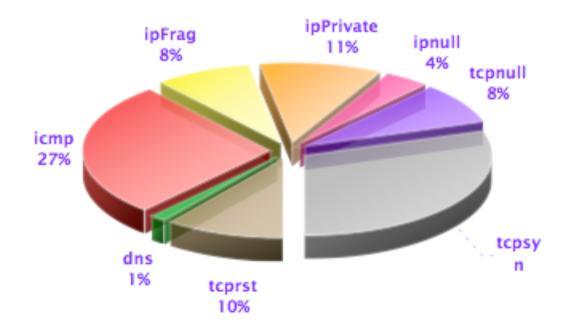
dannyen	over% more food	nts	UT Directon	Access			May 27 2005 10:21	A. 1.4
Туре	over% more food Docume	Start	Durationrector	PPS	BPS	Src	May 27st2005, 10:31	Ports
8	icmp (Outgoing)	03/04/07 19:27:34	11:37 Disk Util	itv1.15 Mpps	549.64 Mbps	xx.xx.0.0/0,xx.xx.0.0/11		
22	topsyn (Outgoing) ovies	03/04/07 19:29:18	11:35 EPSON Se	775.33 Kpps	297.59 Mbps	xx.xx.0.0/0,xx.xx.0.0/3	Apr 2 00.66.73/32	80
22 cts	icmp (Outgoing)	03/04/07 19:29:18	11:35	3.84 Mpps	1.84 Gbps	xx.xx.0.0/0,xx.xx.0.0/3	aa.bb.56.73/32	
10	icmp (Outgoing) Music	03/04/07 19:29:05	9:56 Grab	31.00 Kpps	14.88 Mbps			IVI
16 ⁷ (Lost)	icmp (Outgoing)	03/05/07 02:15:33	4:49 Grapher	273.97 Kpps	131.52 Mbps	xx.xx.0.0/0,xx.xx.0.0/11	Apr 2 aa2bb156.73/321	м
16 tacks	icmp (Outgoing)	03/04/07 19:30:07	4:01 HP Printe	65.13 Kpps	31.26 Mbps	xx.xx.0.0/0,xx.xx.0.0/3	Jan 3, 00.66.73/32	
16andwidt	tcpsyn (Outgoing) ^{ctures}	03/05/07 05:31:16	1:33 Installer	61.97 Kpps	23.79 Mbps	xx.xx.0.0/0,xx.xx.0.0/11	sen 2 aa.bb.56.73/32	- 80
16 ₁₁₀	topsyn (Outgoing)	03/05/07 04:06:16	1:19	57.18 Kpps	21.95 Mbps	xx.xx.0.0/0,xx.xx.0.0/15	aa.bb.56.73/32	80
16	icmp (Outgoing) sf-ppt	03/05/07 01:30:16	32 mins.od Soft	30.48 Kpps	14.63 Mbps	xx.xx.0.0/0,xx.xx.0.0/8	Jul 25 aa.bb.56.73/32	
16	icmp (Outgoing)	03/05/07 00:33:16	49 minsva	27.62 Kpps	13.26 Mbps	xx.xx.0.0/0,xx.xx.0.0/3	Feb 17aa.66.56.73/32	м
[~]	affic:		🕺 🥀 Keychain	Access			Aug 20, 2006, 1:59 A	M
uurnyen	over%10	in the second	Migration	n Assistant			Aug 20, 2006, 6:01 A	M

Internet Attack Packet Size Distribution



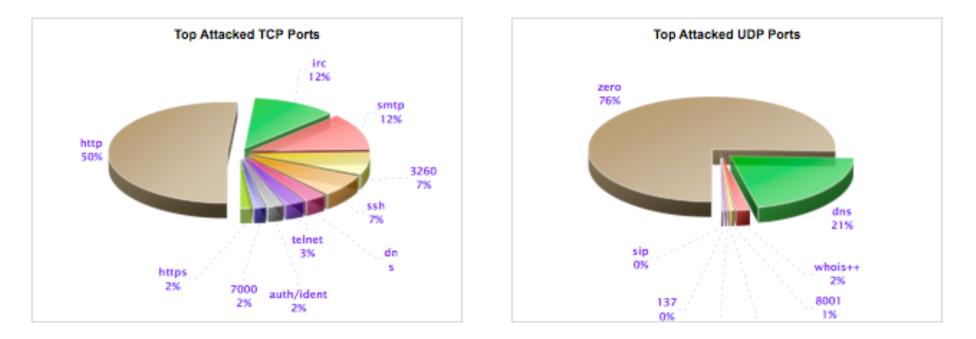
- Small packets predominate (pps attacks)
- Spectral analysis-like fingerprints of other attack types and tools
- Some issues with data collection methodology...

Internet Attack Types



- Data excluding floods
- After nine years, TCP SYN (31%) still dominates DDoS
- ICMP (27%) also prominent

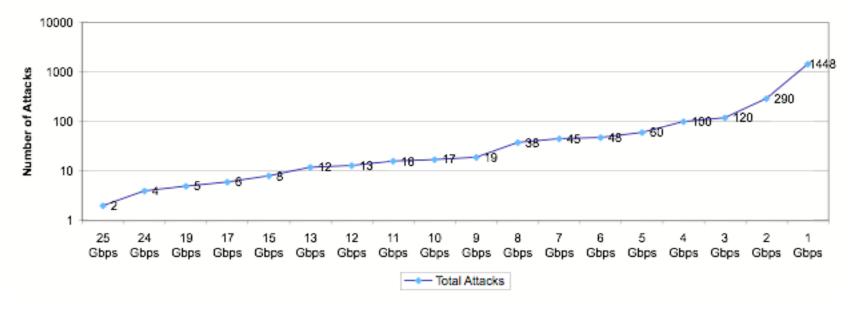
Most Frequently Attacked Ports



- HTTP ports account for bulk of TCP-based attacks
- Fragmentation attacks lead the pack on the UDP front

Internet Attack Scale

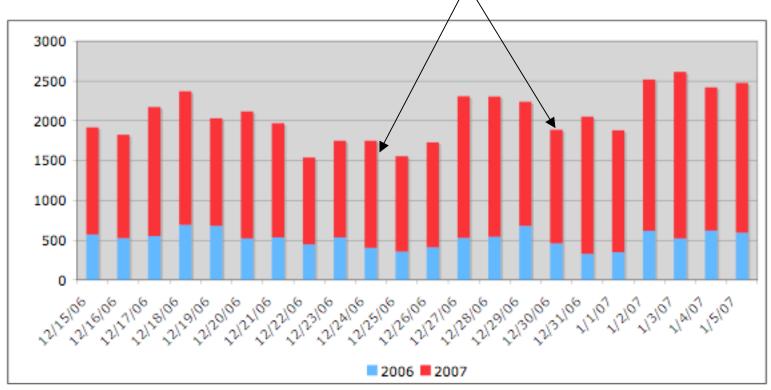
Total Attacks



- Unique attacks exceeding indicated BPS threshold for single ISP
- Average of three 1-Gbps or larger attacks per day over 485 days of collection
- Two ~25 Gbps attacks reported by a single ISP (on same day, about one hour apart, duration of ~35 minutes)

21 Days Y/Y

- Significant Y/Y growth
- Identify additional trends: Holiday Season typically slow time for attackers



Challenges

- Balance commercial privacy with research and business interests
- Data normalization / extrapolation
 - Differing notions tier1
 - Many business units within an ISP
- Data availability to other researchers

Questions?

Craig Labovitz (<u>labovit@arbor.net</u>), Danny McPherson (<u>danny@arbor.net</u>) Scott lekel-Johnson (<u>scottij@arbor.net</u>) Mike Hollyman (mhollyman@arbor.net)