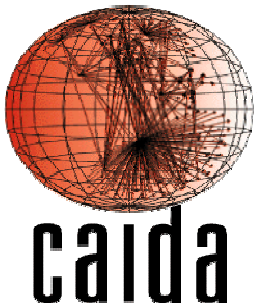
The UCSD Network Telescope

Colleen Shannon
cshannon @ caida.org

NSF CIED Site Visit
November 22, 2004



Motivation

- Blocking technologies for automated exploits is nascent and not widely deployed
  - Research in this area is critical

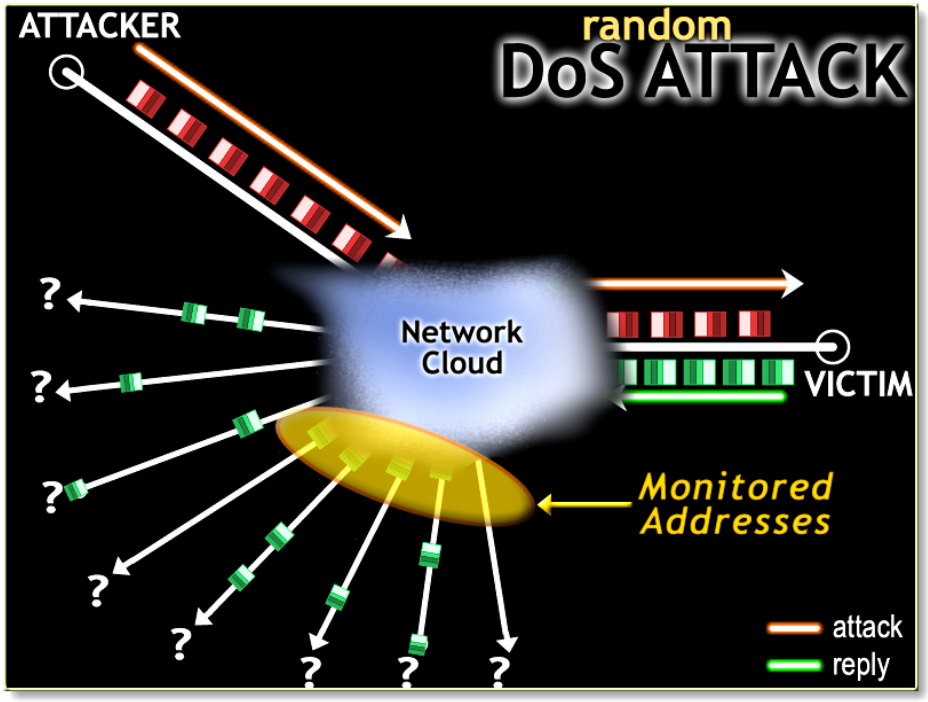
- Measurement of current events complements this research
  - Stay in touch with recent trends (worms are faster and more malicious; botnets are stealthy and widely utilized)
  - Identify new anomalous behavior (whether malicious or simply broken infrastructure)

Network Telescope

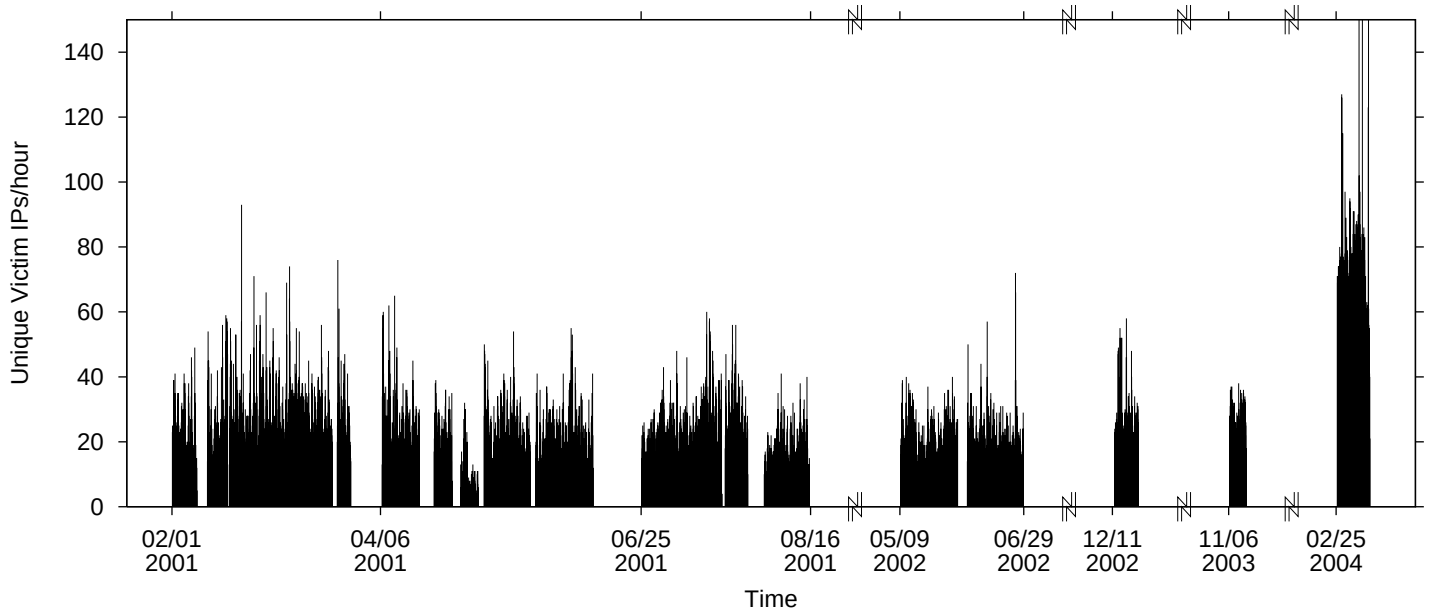
- Chunk of (globally) routed IP address space
- Little or no legitimate traffic (or easily filtered)
- Unexpected traffic arriving at the network telescope can imply remote network/security events
- Generally good for seeing explosions, not small events
- Depends on random component in spread

Network Telescope: Denial-of-Service Attacks

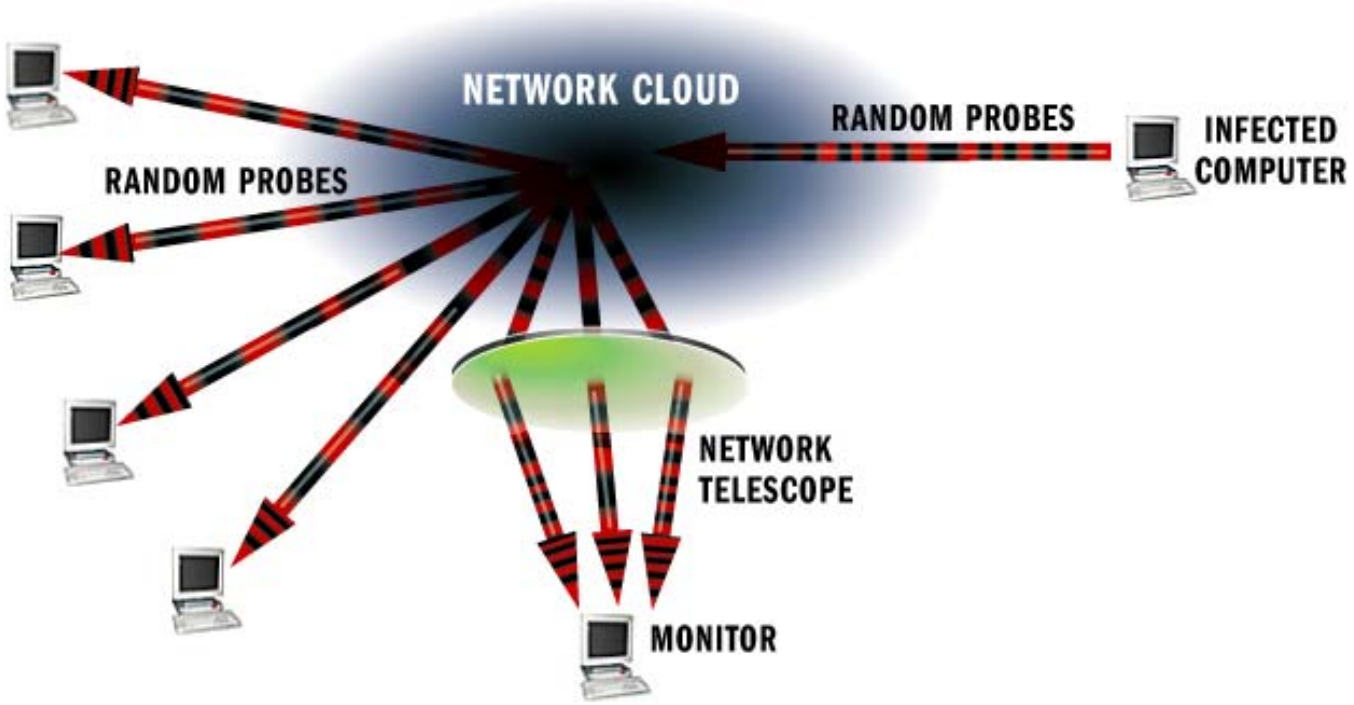
- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- We observe 1/256th of all *victim responses* to spoofed addresses



Denial-of-Service Attacks – Three Years

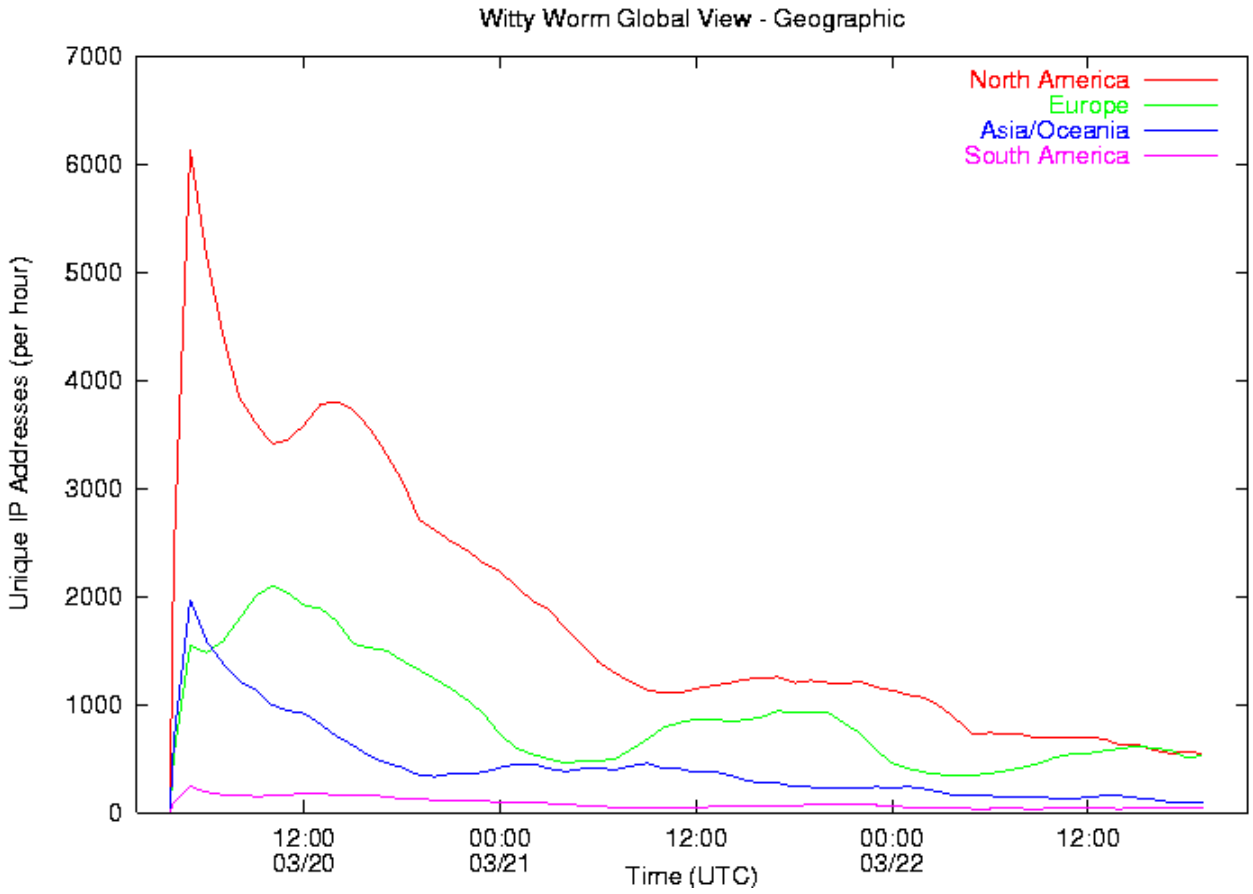


Network Telescope: Worm Attacks



- Infected host scans for other vulnerable hosts by randomly generating IP addresses
- We monitor 1/256th of all IPv4 addresses
- We see 1/256th of all worm traffic of worms with no bias and no bugs

Geographic Spread of Witty



Network Telescope – Current Status

- Continuously collected/archived data
  - 15 months of trace data (Since August 12, 2003)
  - 16 months of flow data (Since July 11, 2003)
  - 0.75 TB/month (8 TB total)
  - 50 researchers currently using February 2001 dataset
- Industry Collaboration
  - Bandwidth Donation
  - Address Space Donations
- Connectivity upgrade

Network Telescope – Bandwidth Donation

- September 2004:
  - Network Telescope is 1/3 of all inbound traffic to UCSD
  - Inbound traffic drives 95th percentile charges
  - Net cost to UCSD for bandwidth: ~$2500/month
- October 2004:
  - Limelight networks donates all inbound connectivity to the UCSD Network Telescope: ~$30,000/year
  - No ports blocked inbound to the Network Telescope

Network Telescope – Address Space Donation

- Current Assets
  - /8 network (Fall 2001)
  - /16 network (Winter 2004)
- Donations in progress
  - Two more /16 networks
  - Five+ /24 networks
- Value in additional address space
  - Interspersed with end user and content hosting networks, increasing the diversity of our view
  - Mix of locally deployed and remotely announced space
  - Accurate epidemiology – who was targeted and when?

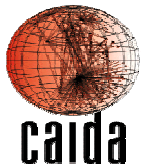
Address Space vs. Detection Time

10 pps events (Code-Red approx. this rate)

Detection probability:	5%	50%	95%
/8 (1 in 256 sampling)	1.3 sec	18 sec	1.3 min
/14	1.4 min	19 min	1.4 hours
/15	3 min	38 min	2.7 hours
/16 (1 in 65,536 sampling)	6 min	1.3 hours	5.5 hours
/19	45 min	10 hours	1.8 days
/24 (1 in ~16.7M sampling)	24 hours	14 days	58 days

Network Telescope – Connectivity Upgrade

- UCSD campus network reconfigured to support:
  - Separate GigE interfaces for all currently monitored address blocks
  - Administrative interface with differently routed path to telescope infrastructure (preserves access during a flash event)
  - Automatic exclusion from UCSD network security measures



Network Telescope - Future

- Honeyfarm deployment
- Traffic characterization for IDS testbed
- PREDICT Data Repository
  - December 2004
- Network Telescope Observation Station
  - Early 2005

DHS Predict Project

- Goal: Get current, relevant (therefore sensitive) network security data to researchers
- ~Six centers around the country coordinating many more data sources (commercial security companies, commercial ISPs, POPs, and co-location/data centers)
- Researchers able to apply for data access in early 2004

DHS Predict Data Distribution

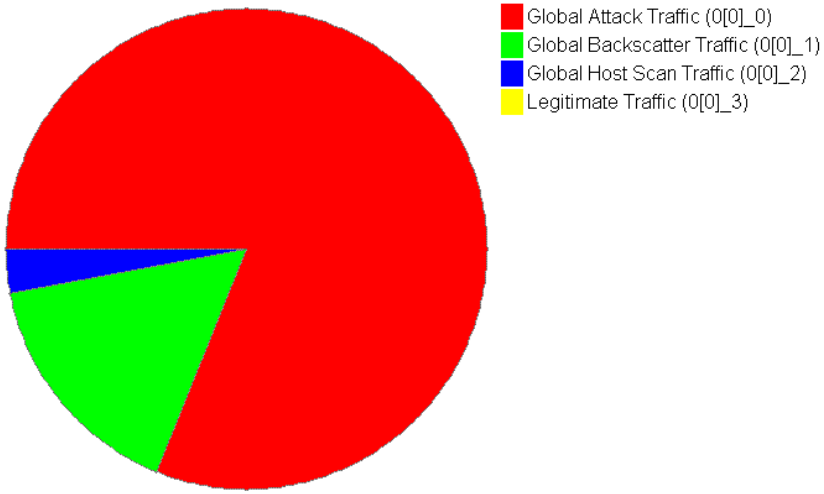
- New Datasets – Coming soon:
  - Code-Red and Witty worm datasets
    - Raw trace data
    - Flow files
    - IP counts over time
    - Hostnames and geographic information
  - 2001-2004 Denial-of-Service backscatter dataset
    - ~One week of data every 3-6 months over 3 years
    - Raw backscatter trace data
    - Attack Flow files
  - (restricted access) Raw telescope traces
- Existing/continuing collections:
  - OC48 traces from large ISPs
  - Active topology measurement data

Network Telescope Observation Station

- Real-time view of Network Telescope activity
  - Publicly accessible
  - Aggregated view protects individual privacy
- Prototype collecting data for more than a year
- Final user interface implementation in progress – Coming soon!

Network Telescope Observation Station

Data by packets from
Network Telescope Observation Station
Mon Nov 22 06:20:45 2004 UTC
300.00s

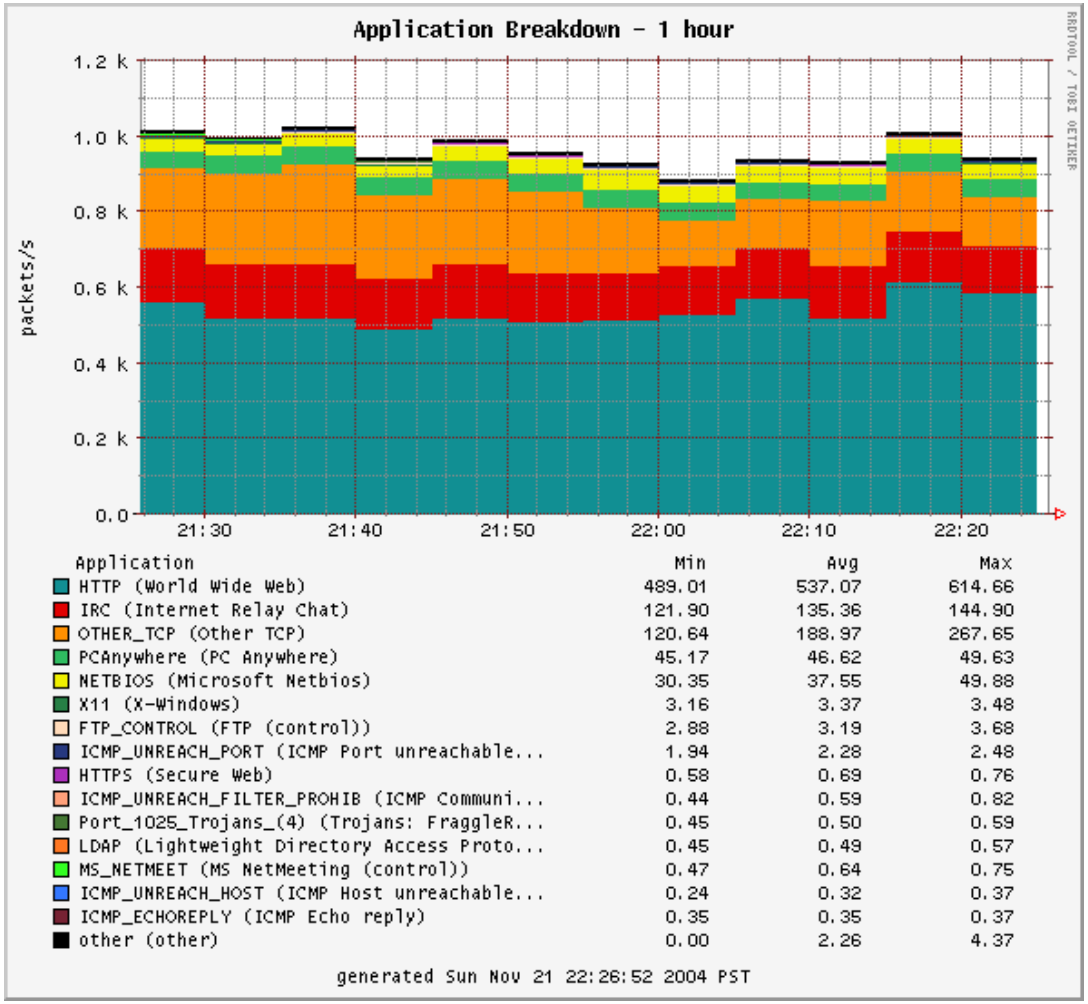


Overall Performance:

Byte rate: 2.4885 Mbits/s
Packet rate: 5.8097 Kpkts/s
Tuple rate: 2707.0967 tuples/s
Total unique subinterface entries: 4 (top 4 by packets shown)

subinterface	Mbits/s	% bytes	Kpkts/s	% packets	tuples/s	% tuples
Global Attack Traffic (0[0]_0)	2.1381	85.92	4.7076	81.03	2133.7967	78.82
Global Backscatter Traffic (0[0]_1)	0.3065	12.32	0.9258	15.94	563.3500	20.81
Global Host Scan Traffic (0[0]_2)	0.0420	1.69	0.1721	2.96	8.4967	0.31
Legitimate Traffic (0[0]_3)	0.0019	0.08	0.0042	0.07	1.4533	0.05

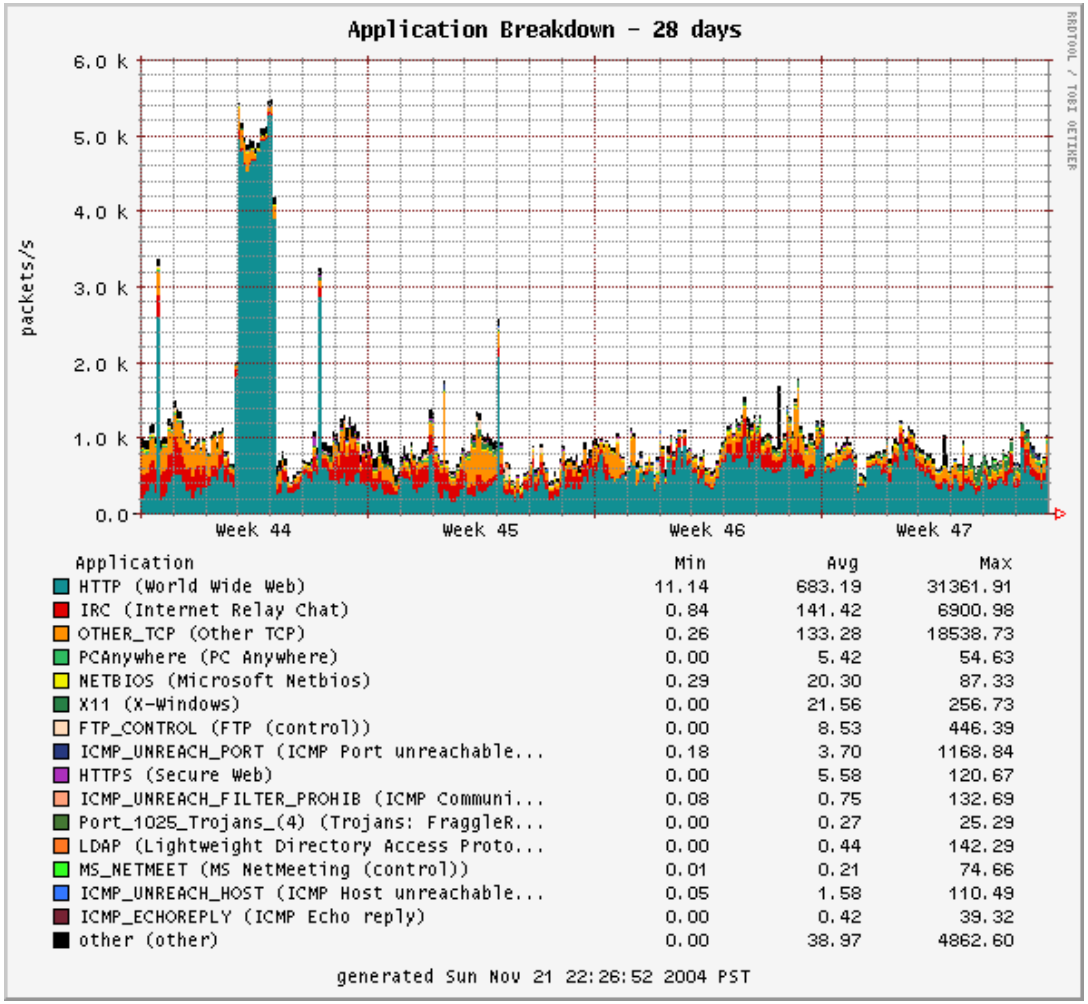
Denial-of-Service Attacks: 1 hour



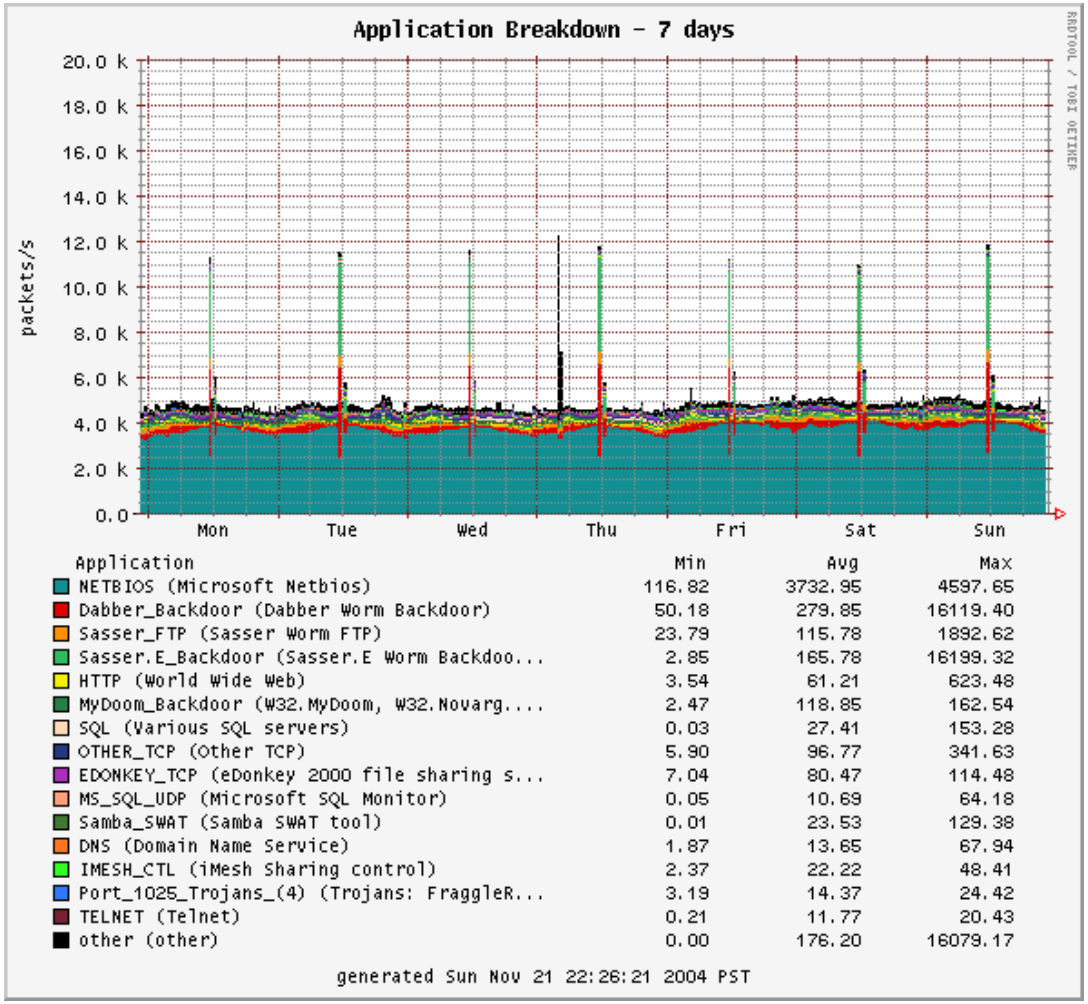
Application	Min	Avg	Max
HTTP (World Wide Web)	489.01	537.07	614.66
IRC (Internet Relay Chat)	121.90	135.36	144.90
OTHER_TCP (Other TCP)	120.64	188.97	267.65
PCAnywhere (PC Anywhere)	45.17	46.62	49.63
NETBIOS (Microsoft Netbios)	30.35	37.55	49.88
X11 (X-Windows)	3.16	3.37	3.48
FTP_CONTROL (FTP (control))	2.88	3.19	3.68
ICMP_UNREACH_PORT (ICMP Port unreachable...	1.94	2.28	2.48
HTTPS (Secure Web)	0.58	0.69	0.76
ICMP_UNREACH_FILTER_PROHIB (ICMP Communi...	0.44	0.59	0.82
Port_1025_Trojans_(4) (Trojans: FraggleR...	0.45	0.50	0.59
LDAP (Lightweight Directory Access Proto...	0.45	0.49	0.57
MS_NETMEET (MS NetMeeting (control))	0.47	0.64	0.75
ICMP_UNREACH_HOST (ICMP Host unreachable...	0.24	0.32	0.37
ICMP_ECHOREPLY (ICMP Echo reply)	0.35	0.35	0.37
other (other)	0.00	2.26	4.37

generated Sun Nov 21 22:26:52 2004 PST

Denial-of-Service Attacks – 1 Month



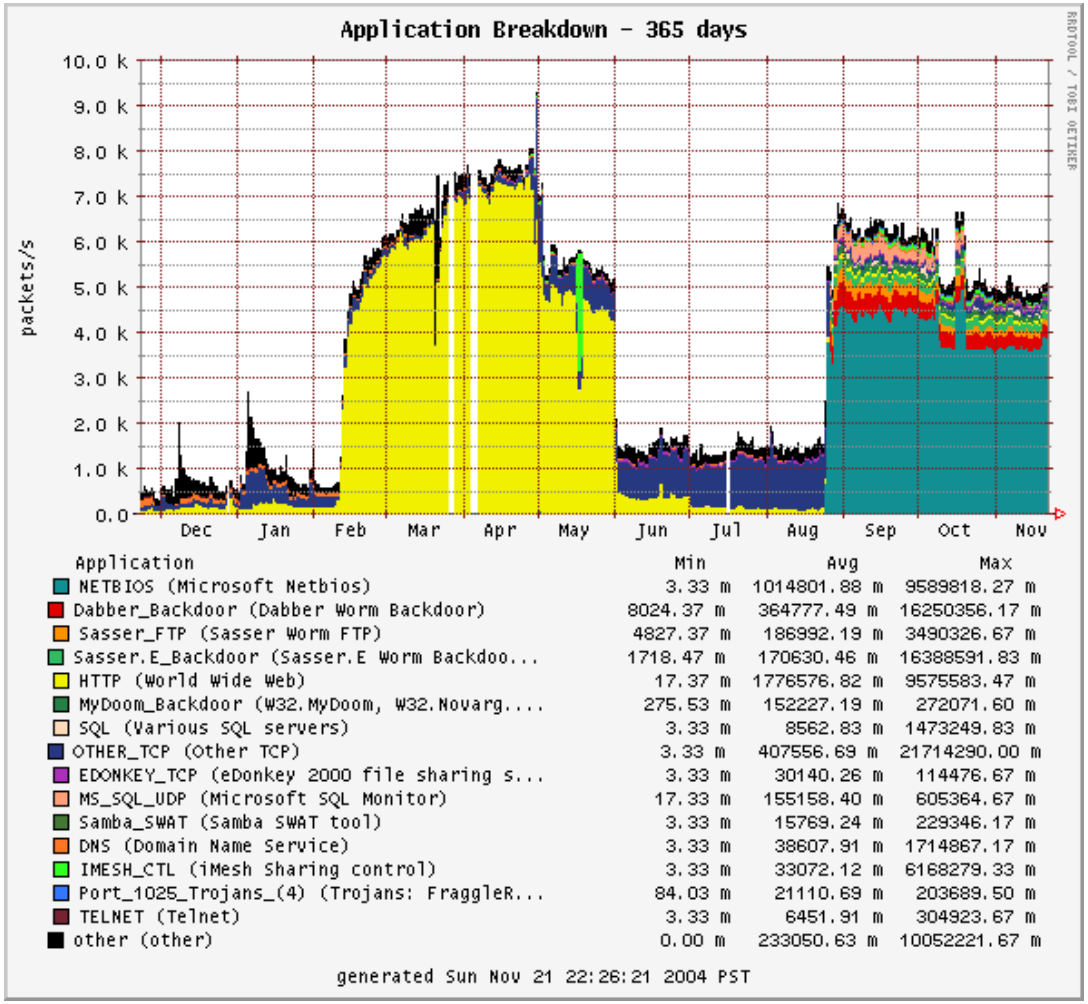
Global Attack Traffic – 1 Week



Application	Min	Avg	Max
NETBIOS (Microsoft Netbios)	116.82	3732.95	4597.65
Dabber_Backdoor (Dabber Worm Backdoor)	50.18	279.85	16119.40
Sasser_FTP (Sasser Worm FTP)	23.79	115.78	1892.62
Sasser.E_Backdoor (Sasser.E Worm Backdoo...	2.85	165.78	16199.32
HTTP (World Wide Web)	3.54	61.21	623.48
MyDoom_Backdoor (W32.MyDoom, W32.Novarg....	2.47	118.85	162.54
SQL (Various SQL servers)	0.03	27.41	153.28
OTHER_TCP (Other TCP)	5.90	96.77	341.63
EDONKEY_TCP (eDonkey 2000 file sharing s...	7.04	80.47	114.48
MS_SQL_UDP (Microsoft SQL Monitor)	0.05	10.69	64.18
Samba_SWAT (Samba SWAT tool)	0.01	23.53	129.38
DNS (Domain Name Service)	1.87	13.65	67.94
IMESH_CTL (iMesh Sharing control)	2.37	22.22	48.41
Port_1025_Trojans_(4) (Trojans: FraggleR...	3.19	14.37	24.42
TELNET (Telnet)	0.21	11.77	20.43
other (other)	0.00	176.20	16079.17

generated Sun Nov 21 22:26:21 2004 PST

Global Attack Traffic – 1 Year



Conclusions

- Active collaborations with UCSD, industry, and research communities paying off
  - Bandwidth
  - Address space
- Community resource: backscatter dataset available; current backscatter and worm datasets coming soon
- Rapid response to current events (SCO DoS attack, Witty Worm)

Acknowledgements

– Technical support of Network Telescope at UCSD:
  - Brian Kantor, Jim Madden, and Pat Wilson

– Support for this work was provided by: NSF, Cisco Systems, DHS, DARPA, and CAIDA members