



<http://www.wowhacker.org>

^^

## DRDoS

---

2002 1 11 2:00am GRC.COM

(DRDoS)

가  
(yahoo.com,

가  
"gary7.nsa.gov"

(router)  
IP

.)

1,072,519,399

(DDoS), TCP , (DRDoS)

(DoS),

---

(Bandwidth Consumption)

1 11

가

가

(flood)

(flood)

가

DDoS  
DDoS

13 "Wicked"

TCP (Transmission Control Protocol) (remote machine) 가

TCP 101 :

가

가 “ ?  
?”

가

가

가 “가 TCP ”

TCP

“ (flag bits)”

“SYN( , synchronize)”

“ACK( , acknowledge)”

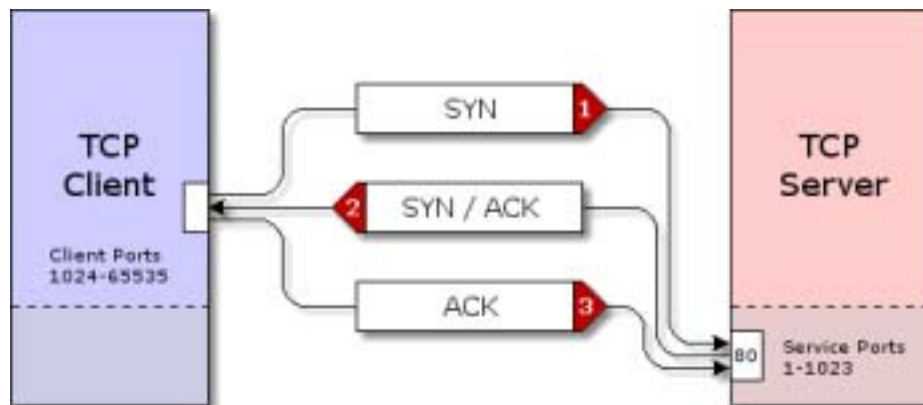
“FIN( , finish)”

TCP

TCP

(Three-Way Handshake)

가



1. SYN : TCP  
TCP

(Client) (ex.

, FTP

)가 “SYN”

SYN

1042

65535

1 1023

가

“

(client)”

”

(ephemeral)”

가

" (service ports)" 80 80  
IP ( IP, The  
IP, The Source IP) 가 ( IP, The  
Destination IP)

2. SYN/ACK: TCP SYN  
"SYN/ACK"  
TCP TCP

"SYN/ACK"

SYN/ACK SYN IP  
SYN/ACK SYN IP  
가

IP 가

가 SYN/ACK 가 가  
가 TCP RST/ACK(Reset Acknowledgement)  
ICMP Port Unreachable

3. ACK: 가 SYN/ACK ACK  
가 SYN/ACK SYN ACK  
TCP

가

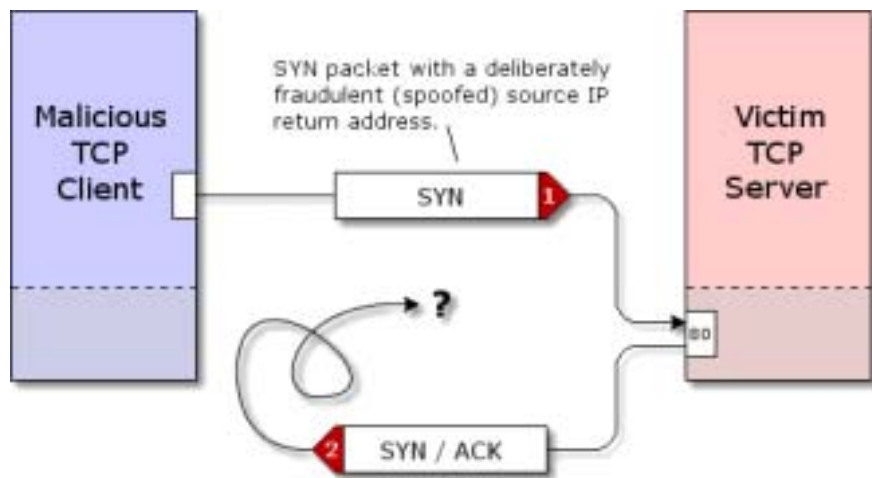
가 ACK SYN/ACK

가

---

TCP : SYN (Flood)  
TCP

TCP 가 SYN  
 IP ACK  
 ACK SYN/ACK  
 SYN 가  
 TCP 가



“ (Raw Sockets)”

“( IP) IP

SYN  
 SYN/ACK

SYN IP ( ) SYN/ACK IP

"RST"(reset)  
 40 가

가

가

가 TCP

SYN

가

가

(operating systems) SYN (Flood)  
 가 (dial-up connection) 가  
 “ (connection queues)” . SYN .

IP SYN .  
 TCP/IP TCP  
 (inbound bandwidth) “ (bandwidth  
 resources)” (connection resources)”가 .

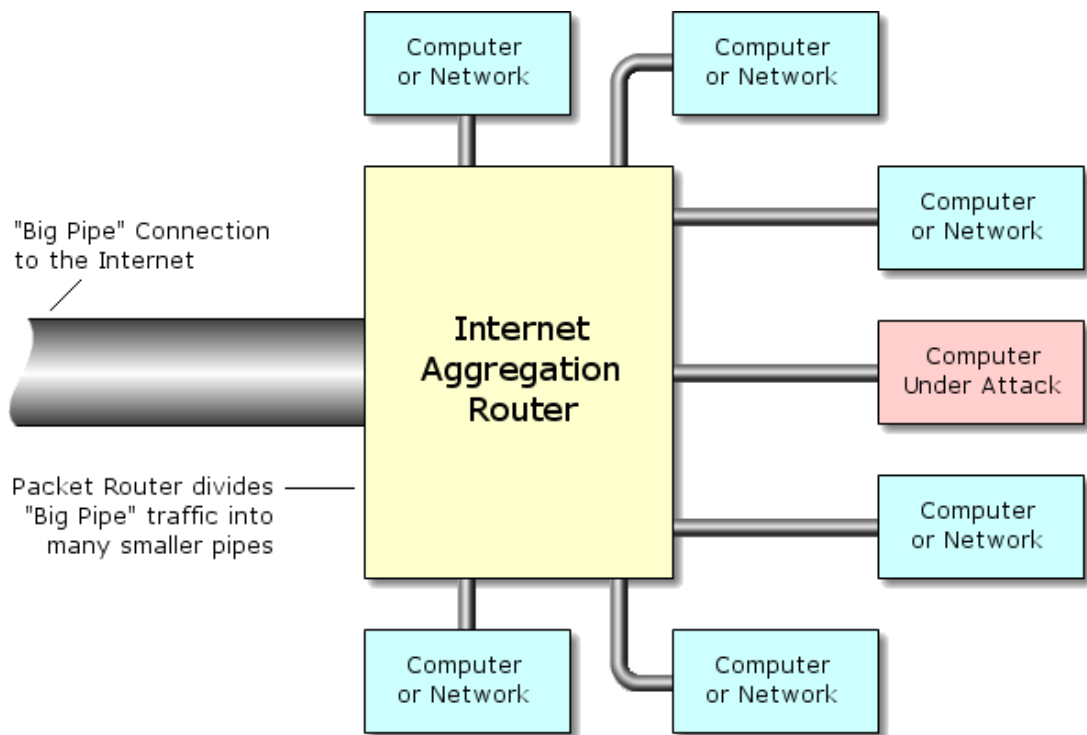
(DoS) . "DDoS" 가 "DoS"  
 가 SYN 가  
 IP SYN .

SYN  
 (Operation System) TCP “  
 (protocol stacks)" SYN DoS .

가 가 : (community)  
 “SYN-cookies” ” (stateless)" TCP .  
 SYN-cookies , “GENESIS”  
 . GENESIS TCP 2000 9 grc.com . DoS  
 가 TCP 가 .  
 SYN SYN/ACK .

---

가  
 “ ” (DDoS) . 가 2001  
 가



“ (aggregation router)” 가

“ (Big Pipe)”

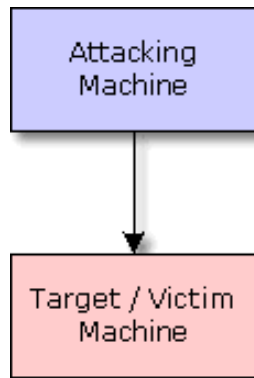
가

---

Dos DDoS

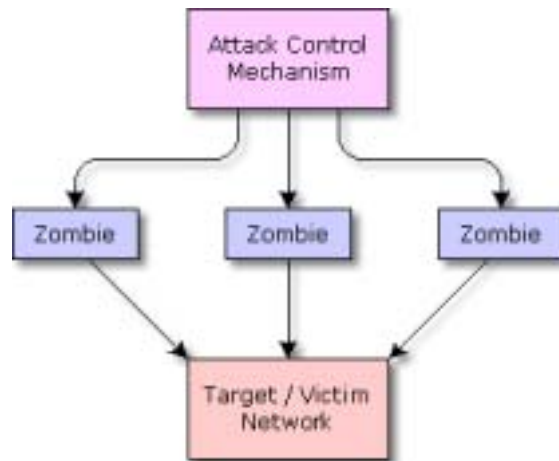
DoS: 가

DoS



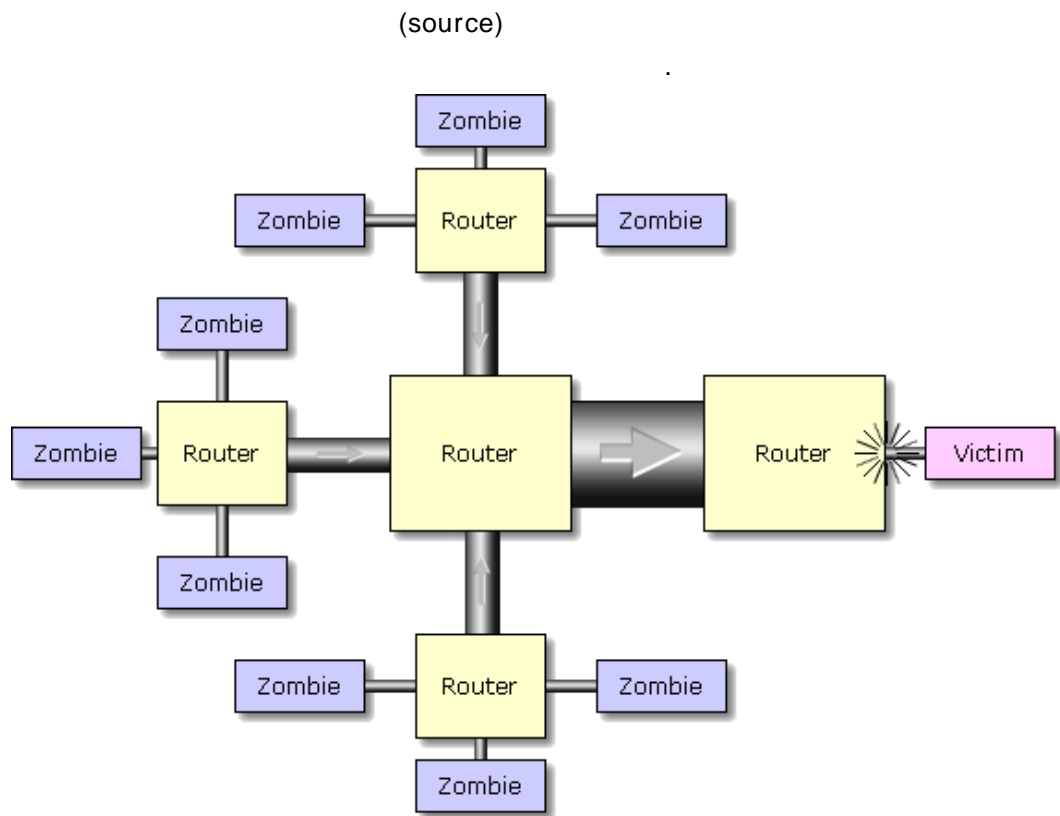
가 (flood) 가

DDoS:  
(flood)



" (Zombie Master)"가 " (Zombie)"가

2001 3 grc.com 13 "Wicked" Windows-hosted Evilbots  
Evilbot IRC Evilgoad



가

## (Distributed Reflection)

DDoS

2002 1 11 2:00 AM grc.com

DDoS

(Distributed

Reflection Denial of Service)

- DRDoS -

2:00

Verio(

)

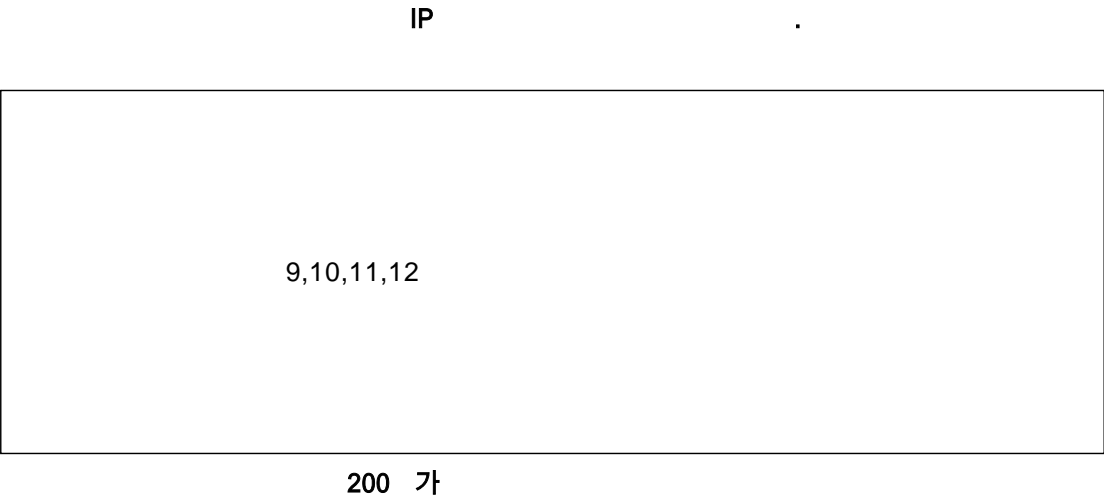
가

T1

(trunk)



(flood)  
0  
Evilbot ( ) UDP ICMP (Window machines)  
(source) IP SYN  
SYN/ACK  
SYN/ACK "ACK" 가 SYN  
“ (raw socket)” 가  
가 ”TCP (flag bits)”

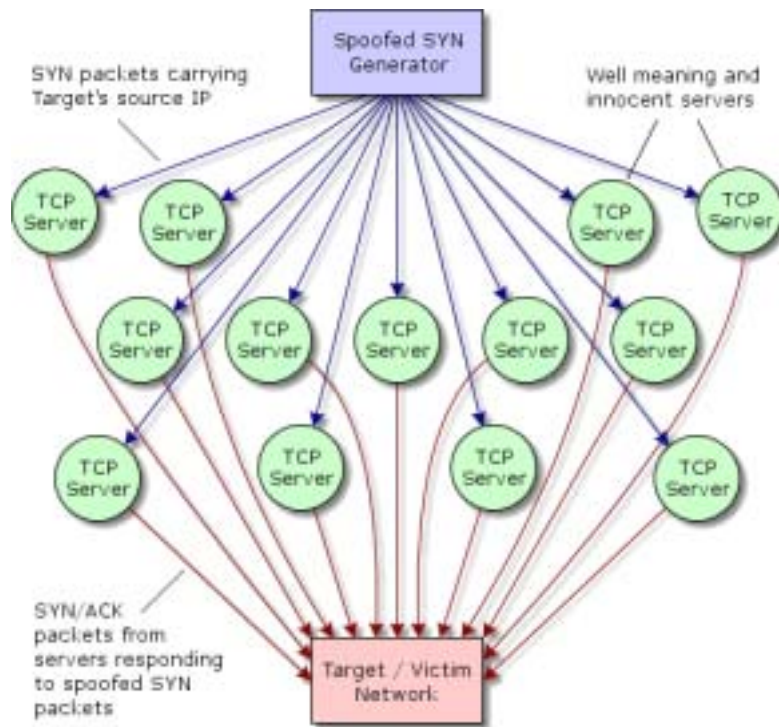


?

Verio, Qwest, Above.net TCP  
179 SYN/ACK  
HTTP 80 179 “BGP”

BGP 가 “ (Border Gateway Protocol)”  
가 IP 가  
“ (routing tables)” BGP

BGP ( 가 )  
179 TCP



가  
TCP  
grc.com  
SYN/ACK  
가  
BGP  
가  
TCP  
SYN  
grc.com  
SYN  
SYN/ACK  
TCP  
SYN  
SYN/ACK  
TCP  
SYN  
SYN/ACK  
TCP  
grc.com

가 .

“ Gibson ”

가 가 . , “ ”  
가 .

가  
Verio .  
4:00가 .  
Verio 24/7 .  
가 .  
Verio 가 .

---

### (reflection attack)

가 , 가 . 가  
가 Verio BGP-equipped 가 .  
SYN BGP 179 .  
179  
Verio (aggregation) “  
” 179 . 179  
(flood) .  
가 .  
! (capture) 가  
traffic (traffic set) 179 router  
traffic 가 router flood  
.(  
.)  
Router traffic , 22(Secure Shell), 23(telnet), 53(DNS),  
80(HTTP/WEF) SYN/ACK .

4001(a proxy server ) 6668(IRC chat)

(flood)

, non-BGP (flooding traffic)

(capture log)

가 BGP

non-BGP SYN/ACK

가

HTTP(web)

80

SYN/ACK

(flooding)

:

Source IP	Machine Name
64.152. 4. 80	www.wwfsuperstars.com
128.121.223.161	veriowebistes.com
131.103.248.119	www.cc.rapidsite.net

164.109. 18.251	whalenstoddard.com
171. 64. 14.238	www4.Stanford.EDU
205.205.134. 1	shell11.novalinktech.net
206.222.179.216	forsale.tx1c.net
208. 47.125. 33	gary7.nsa.gov
216. 34. 13.245	channelserver.namezero.com
216.111.239.132	www.jeah.net
216.115.102. 75	w3.snv.yahoo.com
216.115.102. 76	w4.snv.yahoo.com
216.115.102. 77	w5.snv.yahoo.com
216.115.102. 78	w6.snv.yahoo.com
216.115.102. 79	w7.snv.yahoo.com
216.115.102. 80	w8.snv.yahoo.com
216.115.102. 82	w10.snv.yahoo.com

80 SYN/ACK flooder

가

IP

YAHOO.COM

7

gary7.nsa.gov

..

"Gary7"

Star Trek

.)

가 SYN/ACK TCP BGP  
 179  
 (construction) (consequence)  
 가 (4  
 , ...  
 , Verio router 10 (1,072,519,399) 가 SYN/ACK  
 (BGP가 ) Verio  
 가

---

1/11 , 가,  
 가 ( : high bandwidth)  
 TCP  
 가 , BGP(  
 179) SSH, TELNET, DNS, HTTP IRC  
 “ ”  
 “ ”  
 , 가 , ,  
 “Trace Route” ( )  
 router IP 가 , 가 BGP  
 가 가  
 IP . Yahoo.com  
 가 IP ,  
 TCP , 가  
 IP 가  
 “ ” SYN

SYN/ACK

가 (raw socket)

(Unix, Linux, Windows 2000,

Windows XP)

SYN

SYN

(flooding)

"Bandwidth

( Multiplication" )

가

TCP

SYN

SYN

" "

SYN

TCP

가

SYN 가

" "

SYN (flood)

"SYN flux"

---

가?

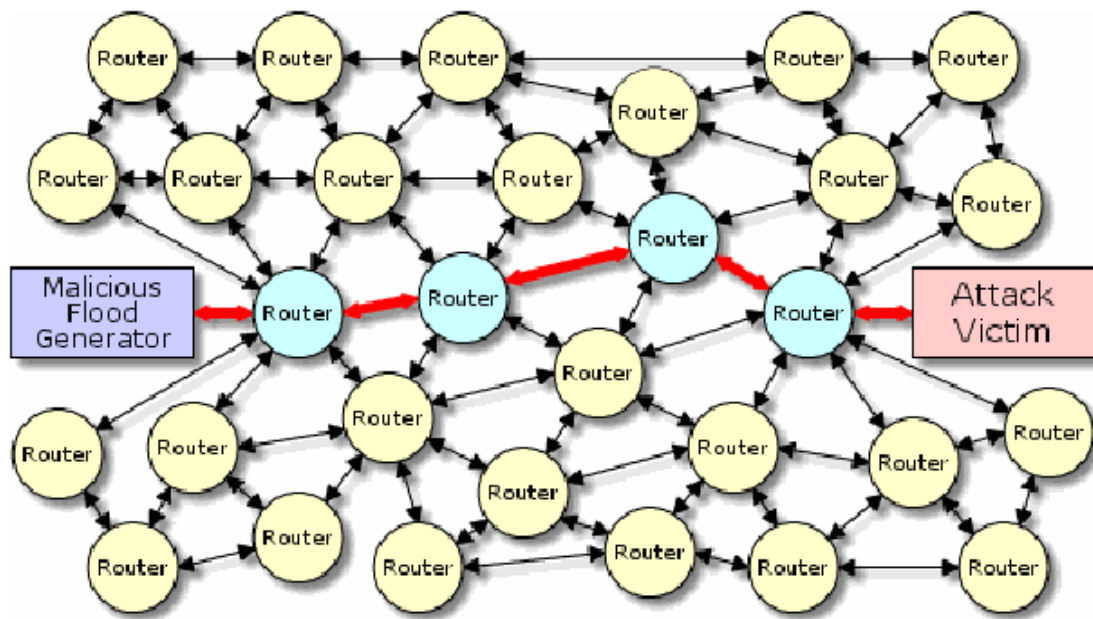
?

TCP

가

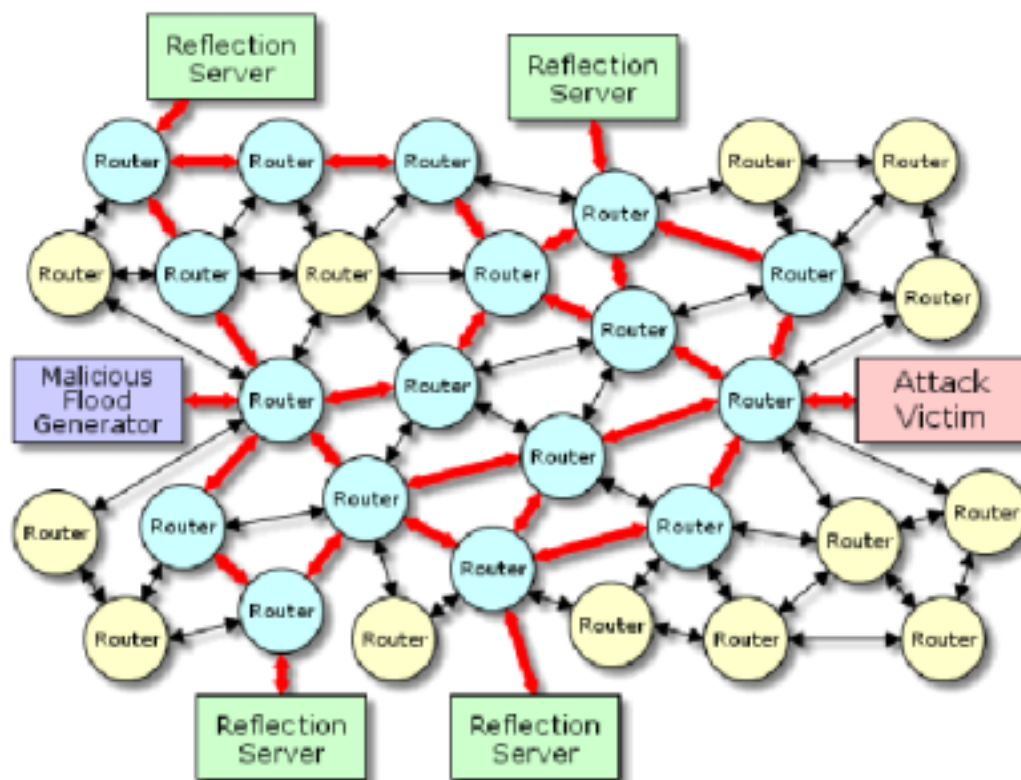
" "

:



가

...



가 , 가  
 , SYN . 가 ,  
 , TCP “ ”  
 가  
 (receiving end) (victim)  
 (attacking machine) (packet flow)  
 , 가  
 (packet flows)  
 (victim) ( .  
 (reflection server) .),  
 (victim)  
 (victim) 가?  
 (victim) 가? SYN/ACK  
 (unwanted) (packet  
 traffic) , (target network) .  
 ...



가 , .

### (Reflector usage phasing)

가  
(inventory)  
(flooding packet) (total  
reflection server inventory) (victim  
network)

“ (reflector usage phasing)”  
(target network)  
(manual nature) ,  
(trickle) (flood) 가  
(intermittent trickle)  
가 가 가

### (Reflector diffusion)

“ ”  
SYN (flood)가 “  
” , SYN  
(half-open) ( 가  
SYN/ACK -  
) , “ (half-open)” TCP  
- (client - aborted  
connections: )

(automated alarm) 가 가  
(ever - changing) (half - open)

( , TCP  
)

### (Bandwidth multiplication)

TCP SYN  
SYN/ACK . TCP가

, SYN  
 SYN/ACK .  
 TCP SYN  
 SYN/ACK (victim) 가  
 (flooding traffic)  
 SYN/ACK  
 ( " " SYN/ACK  
 ( 3 ) (aborted  
 connection)  
 " "  
 가  
 (Improved manageability)  
 DDoS 가 (attacking machines)  
 (required  
 flooding bandwidth)  
 (Stealth)  
 " "  
 가 IP SYN "가 IP"  
 " " IP  
 가 IP IP  
 - - , "  
 " " .( , "  
 (reflection honeypots)"  
 , (DRDoS )  
 가

attack) “ ” IP 80 SYN (flood  
SYN  
SYN\_RECVD-ish 50~100 ) IP 가  
, IP SYN  
(dial-up)  
“ ”, IP 가  
(  
?),  
가  
가  
가 IP( 가 )  
SYN “ ”(flux, )  
SYN  
SYN/ACK “ (flux)”  
가 "SYN\_RECVD"  
SYN (flux) 가  
( ) SYN/ACK  
가  
가  
... IP  
가 가  
IP (flood)  
IRC  
(reflector) IRC  
2 가 (raw header logs)

1 15 ( 가 )

12 IP

IP

1,000,000 가 IP ,

10,000 30,000

가 #23

“ SYN(Stuttering SYN)”

가

SYN “ 12

IP

”

2 3

가 IP가

가 ACK 2

가 가

가 가

IP SYN IP (IP address regions)

“ ”

가

11 SYN

(flood)

2001 11

(flood) SYN/ACK (victim) SYN

가

“ (reflection attack honeypot)”

“ (honeypot)”

IP

IP

“ ”

가

:



( 가 ) TCP  
(  
(low - numbered)

SYN/ACK TCP  
1~1023

가

grc.com 가 4001 6668 SYN/ACK  
SYN/ACK

1024

가

가 SMTP( )

, SMTP

25

SMTP

“ ”  
“ ”

(end user)  
(Client-profile machines)  
(  
가  
가  
가

Bugtraq  
가  
가  
( 가 )”가  
가 “가

SYN IP  
SYN IP  
“ ”

ISP  
가  
ISP  
가  
filtering) ISP  
가 가 ISP  
(egress  
PC 가 (raw

socket) API 가  
Windows XP 가 API 가  
가 ,  
가  
가  
Windows XP ( 가  
) “ ”  
Windows  
Update XP 가

---

가  
“ ”  
가  
TCP  
가  
“ ”  
가  
“ ”(DRDoS)  
TCP

---