

Özgür Yazılımlarla DDOS Saldırılarını Engelleme

Huzeyfe ÖNAL

huzeyfe@lifeoverip.net

<http://www.guvenlikegitimleri.com>



Ben Kimim?

- Bilgi güvenliği Uzmanı(iş hayatı)
- Ağ güvenliği araştırmacısı(gerçek hayat)
- Özgür yazılım destekcisi
 - Hayatını özgür yazılımdan kazanan şanslı insanlardan!
- Kıdemli DDOS uzmanı 😊
- Güvenlik eğitmeni
 - www.guvenlikegitimleri.com
- Günlükcü!
 - www.lifeoverip.net



Neden DDOS Sunumu?

- Gün geçtikçe önemi artan bir konu
- Tehdit sıralamasında en üstlerde
 - En büyük eksiklik temel TCP/IP bilgisi
 - Tecrübesizlik
- DDOS ürünleri çok pahalı
- DDOS ürünleri -eğer onları iyi yapılandırmazsanız- işe yaramaz.
- Özgür yazılımlarla engellenebilecek DDOS saldırılarını analiz etme ve önlem alma...



Ajanda

- Genel tanım ve istatistikler
- DOS/DDOS Saldırı Çeşitleri ve Teknik altyapı
- DOS/DDOS Saldırıları Özgür yazılımlarla analiz etme ve engelleme
 - OpenBSD Packet Filter kullanımı
 - Snort & Ormon & tcpdump kullanımı



Bilinmesi gerekenler...

- Gelen DDOS saldırısı sizin sahip olduğunuz bantgenişliğinden fazlaysa yapılabilecek çok şey yok!
- DDOS saldırılarının büyük çoğunluğu bantgenişliği taşıma şeklinde gerçekleşmez!

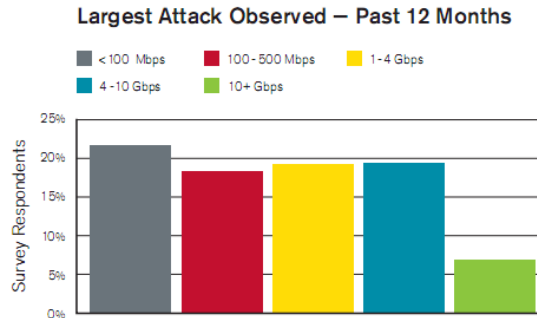


Figure 5: Largest Attack Observed – Past 12 Months
Source: Arbor Networks, Inc.

**Gürcistan DDOS saldırısı
200-800 Mbps arası**



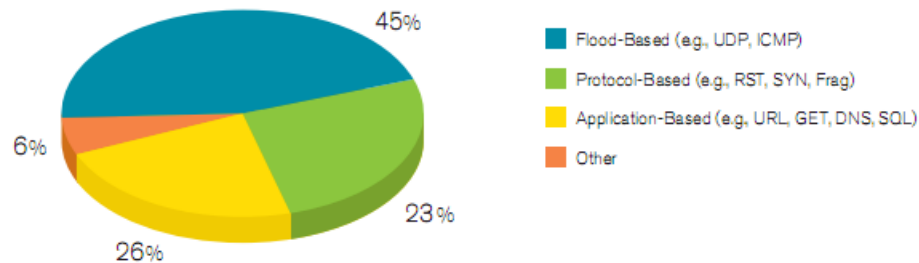
Terimler

- IP Spoofing
- DOS
- DDOS
- SYN, FIN, ACK, PUSH ...
- BotNet
- Flood
- RBN(Russian Business Network)



DOS/DDOS Saldırı İstatistikleri

Largest Observed Attack Vectors



Largest Attack Observed – Past 12 Months

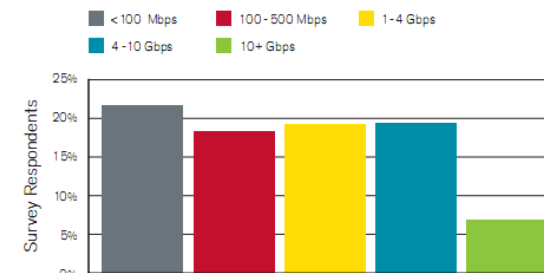


Figure 5: Largest Attack Observed – Past 12 Months

Source: Arbor Networks, Inc.

Primary Attack Mitigation Techniques

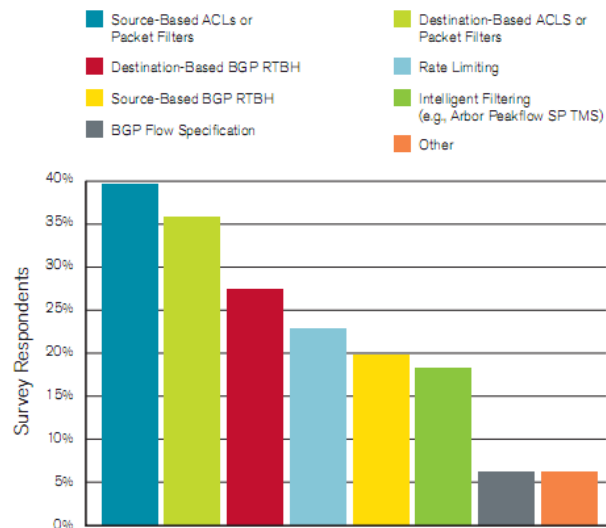
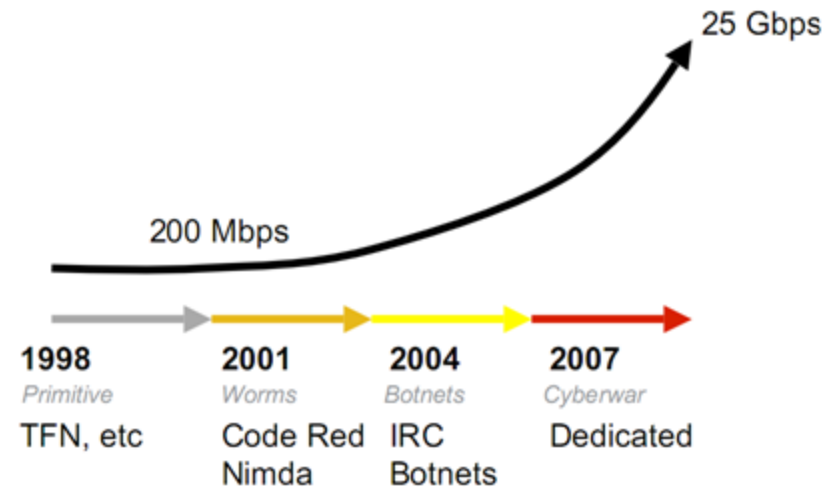


Figure 9: Primary Attack Mitigation Techniques

Source: Arbor Networks, Inc.



Güncel DDOS Örnekleri



Gerçek Hayattan DDOS Örnekleri

- Karşılaştığım saldırıların “en” leri...
- En uzun DDOS saldırısı: 4 gün
- En yüksek kapasiteli saldırı 2.5 Gb
- En komik DOS saldırısı: 2Mb ile 1Gb’lik hattı indirme
- En etkili DOS saldırısı :Bind DOS



Kimler Neden Yapar?

- Ev kullanıcıları (ADSL vs)
 - Küçük sitelere HTTP GET Flood şeklinde
 - Genelde tehlikesizdirler
- Hackerlar/Profesyoneller
 - Botnet oluştururken sadece son kullanıcılardan değil, sunucu sistemlerden faydalanırlar
 - Bir sunucu ~1000 istemci gücünde trafik üretebilir
 - Özellikle Linux sunuculardaki güvenlik açıklıkları çok kullanılır
- Elllerinde sağlam kaynaklar vardır
 - Bazıları bu kaynakları satar(RBN)
 - Günlük 10 Gb atak 300 \$ vs



Ne kadar zordur?

Stats botnet

Refresh Clear stats

Stats Bots

All bots: 6
ONLINE: 6
OFFLINE: 0
Free: 6
Work: 0
Country: 1

List bots

Search bot (mask: id, ip, country):

ID	Ver	Country	IP	Status	First time	Last time
1	4	Brazil		Free	2009-01-08 00:22:32	2009-01-08 08:37:20
2	4	Canada		Free	2009-01-08 00:41:10	2009-01-08 08:37:20
3	4	Thailand		Free	2009-01-08 04:33:12	2009-01-08 08:37:20
4	4	Kyrgyzstan		Free	2009-01-08 06:03:39	2009-01-08 08:37:20
5	4	Russian Federation		Free	2009-01-08 06:10:46	2009-01-08 08:37:20
6	4	Georgia		Free	2009-01-08 08:02:13	2009-01-08 08:37:20

Create new task

Host[:port]:
Path:
Referrer:
POST:
Bots:
Type:
Status:
Start:
End:

Add Cancel

Page 1 of 1 View tasks Displaying 1 - 6 of 6

Zeus :: Statistics - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

in.php?m=home 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

template for SPAM task

template:

Enter name new template and upload files attach.
- Uploaded .txt file for text mail.
- Uploaded .html, .htm file for html mail.
If html mail used image, css - upload auto attach in mail, and used name into html.
And upload pdf, zip, rar, doc, xls and etc. for attach in mail.

Update build

Version: 4
File: Select file
Update

DOS/DDOS Çeşitleri

- Bandwidth şişirme
 - Udp flood, icmp flood (diğer tüm tipler)
- Kaynak tüketimi(Firewall, server)
 - Synflood, ACK/FIN flood, GET/POST Flood, udp flood
- Programsal hata
 - Bind DOS
- Protokol istismarı
 - DNS amplification DOS
- Spoof edilmiş IP kullanılmış mı ?....



DDOS-1:Bandwidth Şişirme

- Önlemenin yolu yoktur
 - Sürahi bardak ilişkisi
- ISP seviyesinde engellenebilir...
- L7 protokolleri kullanılarak yapılan DDOS'larda saldırı trafiği çeşitli yöntemlerle ~6'da birine düşürülebilir
 - HTTP GET flood 400 Byte
 - IP Engelleme sonrası sadece syn 60 byte



DDOS-II:Ağ/güvenlik cihazlarını yorma

- Amaç ağ-güvenlik sistemlerinin kapasitesini zorlama ve kaldıramayacakları kadar yük bindirme
- Session bilgisi tutan ağ/güvenlik Cihazlarının kapasitesi sınırlıdır



Biraz TCP/IP bilgisi...

- Saldırılarda kullanılan paket çeşitleri ve boyutları



TCP SYN Paketi

Ortalama 60 byte

```
[root@mail ~]# hping -p 80 -S 99.99.99.1 -c 1
HPING 99.99.99.1 (bcel 99.99.99.1): S set, 40 headers + 0 data bytes

--- 99.99.99.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@mail ~]#
```

```
mail.lifeoverip.net - SecureCRT
File Edit View Options Transfer Script Tools Help

mail.lifeoverip.net
[root@mail ~]# tcpdump -i bcel -v -s0 -tn host 99.99.99.1
tcpdump: listening on bcel, link-type EN10MB (Ethernet) capture size 65535 bytes
IP (tos 0x0, ttl 64, id 16922, offset 0, flags [none], proto TCP (6), length 40)
  91.93.119.80.2636 > 99.99.99.1.80: Flags [S], cksum 0xfeae (correct), seq 156218608, win 512, length 0
```

Gönderilen her SYN paketi için hedef sistem ACK-SYN paketi üretecektir.



UDP Paket Boyutu

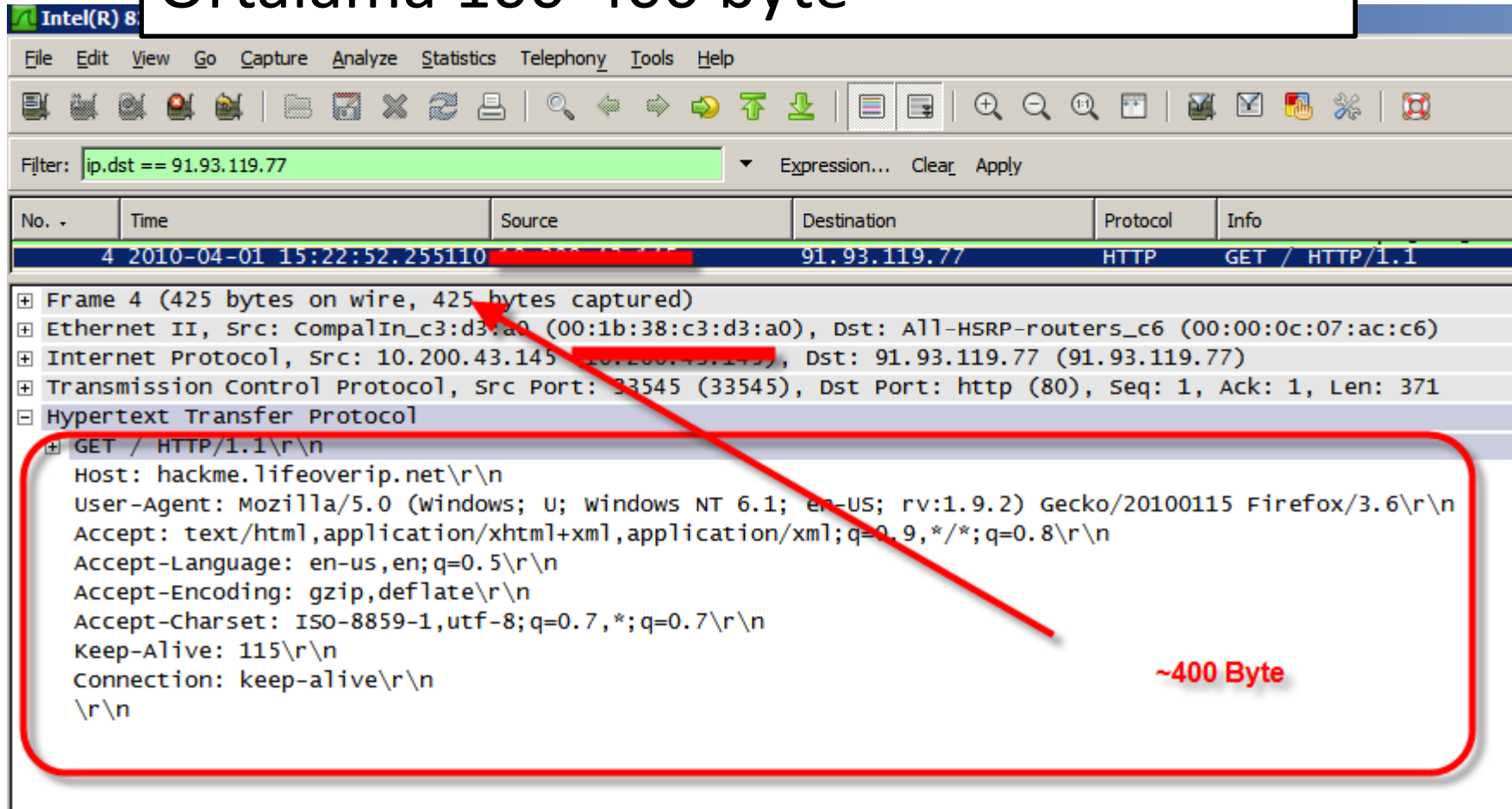
Ortalama 30 byte

```
[root@mail ~]#  
[root@mail ~]#  
[root@mail ~]# hping -p 53 --udp 99.99.99.1 -c 1  
HPING 99.99.99.1 (bcel 99.99.99.1): udp mode set, 28 headers + 0 data bytes  
  
--- 99.99.99.1 hping statistic ---  
1 packets tramitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@mail ~]#  
  
mail.lifeoverip.net - SecureCRT  
File Edit View Options Transfer Script Tools Help  
  
mail.lifeoverip.net  
[root@mail ~]# tcpdump -i bcel -v -s0 -tn host 99.99.99.1  
tcpdump: listening on bcel, link-type EN10MB (Ethernet), capture size 65535 bytes  
IP (tos 0x0, ttl 64, id 54669, offset 0, flags [none], proto UDP (17), length 28)  
91.93.119.80.2808 > 99.99.99.1.53: [|domain]
```



HTTP GET Paket Boyutu

Ortalama 100-400 byte



Filter: `ip.dst == 91.93.119.77`

No.	Time	Source	Destination	Protocol	Info
4	2010-04-01 15:22:52.255110	10.200.43.145	91.93.119.77	HTTP	GET / HTTP/1.1

Frame 4 (425 bytes on wire, 425 bytes captured)

- Ethernet II, Src: CompalIn_c3:d3:a0 (00:1b:38:c3:d3:a0), Dst: All-HSRP-routers_c6 (00:00:0c:07:ac:c6)
- Internet Protocol, Src: 10.200.43.145 (10.200.43.145), Dst: 91.93.119.77 (91.93.119.77)
- Transmission Control Protocol, Src Port: 33545 (33545), Dst Port: http (80), Seq: 1, Ack: 1, Len: 371
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: hackme.lifeoverip.net\r\n
 - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 - Accept-Language: en-us,en;q=0.5\r\n
 - Accept-Encoding: gzip,deflate\r\n
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
 - Keep-Alive: 115\r\n
 - Connection: keep-alive\r\n
 - \r\n

~400 Byte



100-1000 Mb ile neler yapılabilir?

- Saldırı Tipine göre
 - SYN Flood olursa
 - [100 Mb 200.000 pps]
 - [1Gb 2.000.000 pps]
 - UDP flood olursa
 - [100Mb 400.000pps]
 - [1Gb 4.000.000 pps]
 - GET Flood olursa
 - [100Mb 32.000 pps]
 - [1Gb 320.000 pps]



Firewall Timeout Değerleri

```
[root@mail ~]# pfctl -st
No ALTQ support in kernel
ALTQ related functions disabled
tcp.first          120s
tcp.opening        30s
tcp.established    86400s
tcp.closing        900s
tcp.finwait        45s
tcp.closed         90s
tcp.tsdiff         30s
udp.first          60s
udp.single         30s
udp.multiple       60s
icmp.first         20s
icmp.error         10s
other.first        60s
other.single       30s
other.multiple     60s
frag              30s
interval           10s
adaptive.start     1800000 states
adaptive.end       3600000 states
src.track          0s
[root@mail ~]#
```



Günümüz “Enterprise Security” Ürünleri

- Saldırganın silahlarını ve gücünü gördük, buna karşılık güvenlik dünyasının ürettiği savunma sistemlerinin özelliklerine ve güçlerine bakalım
- Firewall/IPS sistemleri DDOS saldırılarına karşılık kadar dayanıklı....
 - Gelebilecek itirazlar: Firewall/IPS sistemleri DDOS engelleme amaçlı değildir(!)



Fortinet Firewall Limitleri

Technical Specifications

HARDWARE SPECIFICATIONS

	FortiGate-1000A	FortiGate-1000AFA2	FortiGate-3016B	FortiGate-3600A	FortiGate-3810A
10/100/1000 Interfaces (Copper)	10	10	8	8	8
1Gb SFP Interfaces	0	0	0	0	2 - 26*
SFP Transceivers Provided	NA	NA	NA	NA	2 (SX)
USB Ports	1	1	1	1	1
AMC Expansion Slots	0	0	0	0	2 single width 2 double width

SYSTEM PERFORMANCE

Concurrent Sessions	1,100,000	1,100,000	1,100,000	1,100,000	2,000,000
New Sessions/Second	15,000	15,000	15,000	15,000	40,000
Firewall Throughput (Gbps)	2 Gbps	2 Gbps	16 - 20* Gbps	6 - 10* Gbps	7 - 37* Gbps
VPN Throughput (IPSec)	600 Mbps	600 Mbps	12 - 15* Gbps	0.8 - 3.8* Gbps	1 - 19* Gbps
IPS Throughput	1 Gbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps
Antivirus Throughput	200 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Unlimited Concurrent Users	Yes	Yes	Yes	Yes	Yes
Site-to-site IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000
Client-to-Site IPSec VPN Tunnels	10,000	10,000	64,000	64,000	64,000
Number of Concurrent SSL Users (Recommended)	1,000	1,000	2,000	3,000	5,000
Policies	100,000	100,000	100,000	100,000	100,000
Virtual Domains (VDOMS) (standard / with optional license)	10 / NA	10 / NA	10 / 250	10 / 250	10 / 250

20Mb hat=40.000 pps
(20x1024x1024/8/60)
50 saniyede 2.000.000 session



Netscreen Firewall Limitleri



NETSCREEN-5200



NETSCREEN-5400

Specifications

	NETSCREEN-5200	NETSCREEN-5400
Maximum Performance and Capacity¹		
ScreenOS® version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets) ²	10/8 Gbps	30/24 Gbps
Firewall performance (small packets)	4 Gbps	12 Gbps
Firewall Packets Per Second (64 byte)	6 M PPS	18 M PPS
AES256+SHA-1 VPN performance ²	5/4 Gbps	15/12 Gbps
3DES+SHA-1 VPN performance ²	5/4 Gbps	15/12 Gbps
Maximum concurrent sessions ³	1,000,000	2,000,000 ⁽⁹⁾
New sessions/second ¹⁰	26,500/22,000	26,500/22,000



Netscreen ISG Limitleri



	ISG1000	ISG2000
Maximum Performance and Capacity¹		
ScreenOS® version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets)	2 Gbps	4 Gbps
Firewall performance (small packets)	1 Gbps	2 Gbps
Firewall packets per second (64 byte)	1.5 M PPS	3 M PPS
AES256+SHA-1 VPN performance	1 Gbps	2 Gbps
3DES+SHA-1 VPN performance	1 Gbps	2 Gbps
Maximum concurrent sessions ³	500,000	1,000,000
New sessions/second	20,000	23,000
Maximum security policies	10,000	30,000



Checkpoint Power-1 Limitleri

Check Point Power-1 Appliances

Security for high-performance environments



Power-1 11000 series



Power-1 5075



Power-1 9075

Hardware Specifications

Hardware Specifications

Appliance	Power-1 5075	Power-1 9075	Power-1 11000 Series		
			11065	11075	11085
Software Edition	R65, R70	R65, R70	R70	R70	R70
Operating System	Secure Platform	Secure Platform	Secure Platform	Secure Platform	Secure Platform
10/100/1000 Ports	10/14	14/18	14/18	14/18	14/18
10Gb ports	2 optional	4 optional	4 optional	4 optional	4 optional
Firewall Throughput ¹	9 Gbps	16 Gbps	15 Gbps	20 Gbps	25 Gbps
VPN Throughput ¹	2.4 Gbps	3.7 Gbps	3.7 Gbps	4 Gbps	4.5 Gbps
Concurrent Sessions	1.2 Million	1.2 Million	1.2 Million	1.2 Million	1.2 Million



TippingPoint 10Gb IPS Limitleri

data_sheet

TippingPoint_N-Platform

Technical Specifications

Hardware	TippingPoint 660N	TippingPoint 1400N	TippingPoint 2500N	TippingPoint 5100N
Performance				
Inspected Throughput ¹	750 Mbps	1.5 Gbps	3 Gbps	5 Gbps
Network Throughput ²	750 Mbps	1.5 Gbps	15 Gbps	15 Gbps
Typical Latency ³	< 80 microseconds	< 80 microseconds	< 80 microseconds	< 80 microseconds
Concurrent Network Sessions ⁴	6,500,000	6,500,000	10,000,000 ⁵	10,000,000 ⁵
Security Contexts ⁶	1,200,000	1,200,000	2,800,000	2,800,000
Connections Per Second	115,000	115,000	230,000	230,000
Scalability				
Interfaces	1 GbE	1 GbE	10 GbE	10 GbE
Ethernet Ports	(20) 10/100/1000	(20) 10/100/1000	(2) 10 GbE XFP	(2) 10 GbE XFP
Port Quantity/Type	(10) Copper/(10) SFP	(10) Copper/(10) SFP	(2) 10 GbE XFP	(2) 10 GbE XFP
Number of Port Segments	10	10	1	1
Zero Power HA	External	External	Modular	Modular
			External	External



DDOS-III:Programlama Hatası:ISC Bind

BIND Dynamic Update DoS

BIND denial of service (server crash) caused by receipt of a specific remote dynamic update

CVE: [CVE-2009-0696](#)

CERT: [VU#725188](#)

Posting date: 28 Jul 2009

Program Impacted: BIND

Versions affected: BIND 9 (all version)

Severity: High

Exploitable: remotely

Description:

Urgent: this exploit is public. Please upgrade immediately.

Receipt of a specially-crafted dynamic update message to a zone for which the server is the master may cause BIND 9 servers to exit. Testing indicates that the attack packet has to be formulated against a zone for which that machine is a master. Launching the attack against slave zones does not trigger the assert.

This vulnerability affects all servers that are masters for one or more zones – it is not limited to those that are configured to allow dynamic updates. Access controls will not provide an effective workaround.

dns_db_findrdataset() fails when the prerequisite section of the dynamic update message contains a record of type "ANY" and where at least one RRset for this FQDN exists on the server.

```
db.c:659: REQUIRE(type != ((dns_rdatatype_t)dns_rdatatype_any)) failed
exiting (due to assertion failure).
```

Workarounds:

None.

(Some sites may have firewalls that can be configured with packet filtering techniques to prevent nsupdate messages to nameservers.)

Active exploits:

An active remote exploit is in wide circulation at this time.

Tek paketle DNS sunucuyu
durdurma saldırısı

```
[root@netdos1 ~]# perl bind_dos.pl -a 99.99.99.1 -d 91.93.119.80
;; HEADER SECTION
;; id = 32303
```

%85 DNS sunucusu ISC Bind



DDOS-IV:Protokol İstismarı(DNS DOS)

- Amplification saldırısı
 - Çarşıdan aldık bir byte eve geldik 10 byte...
- Sahte DNS istekleriyle servis yorma
 - Saniyede 50.000 dns isteği ve olmayan domainler için...

```
root@guvenlikod: ~  
root@guvenlikod:~# dig . @gezginler.net  
  
;<<>> DiG 9.5.0-P2 <<>> . @gezginler.net  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54348  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14  
;; WARNING: recursion requested but not available  
  
;; QUESTION SECTION:  
; . IN A  
  
;; AUTHORITY SECTION:  
347143 IN NS h.root-servers.net.  
347143 IN NS i.root-servers.net.  
347143 IN NS j.root-servers.net.  
347143 IN NS k.root-servers.net.  
347143 IN NS l.root-servers.net.  
347143 IN NS m.root-servers.net.  
347143 IN NS a.root-servers.net.  
347143 IN NS b.root-servers.net.  
347143 IN NS c.root-servers.net.  
347143 IN NS d.root-servers.net.  
347143 IN NS e.root-servers.net.  
347143 IN NS f.root-servers.net.  
347143 IN NS g.root-servers.net.  
  
;; ADDITIONAL SECTION:  
a.root-servers.net. 347143 IN A 198.41.0.4  
a.root-servers.net. 347143 IN AAAA 2001:503:ba3e::2:30  
b.root-servers.net. 347143 IN A 192.228.79.201  
c.root-servers.net. 347143 IN A 192.33.4.12  
d.root-servers.net. 347143 IN A 128.8.10.90  
e.root-servers.net. 347143 IN A 192.203.230.10  
f.root-servers.net. 347143 IN A 192.5.5.241  
f.root-servers.net. 347143 IN AAAA 2001:500:2f::f  
g.root-servers.net. 347143 IN A 192.112.36.4  
h.root-servers.net. 347143 IN A 128.63.2.53  
h.root-servers.net. 347143 IN AAAA 2001:500:1::803f:235  
i.root-servers.net. 347143 IN A 192.36.148.17  
j.root-servers.net. 347143 IN A 192.58.128.30  
j.root-servers.net. 347143 IN AAAA 2001:503:c27::2:30  
  
;; Query time: 176 msec  
;; SERVER: 208.43.98.30#53(208.43.98.30)  
;; WHEN: Fri Mar 12 05:58:09 2010  
;; MSG SIZE rcvd: 500
```

Istek 45 byte
Cevap 528 byte

10Mb hat ile 120 Mb
UDP trafigi
olusturulabilir.
(10*1024*1024/45)*



Saldırı Çeşitleri ve Korunma Yolları



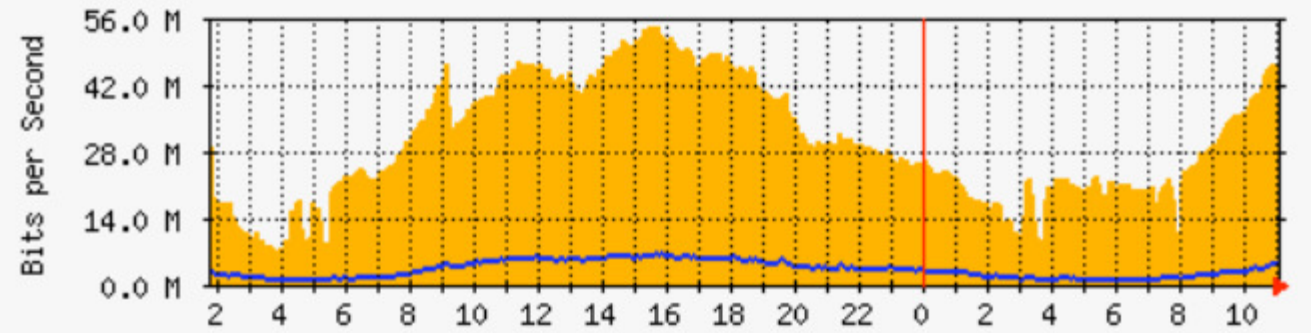
DDOS Saldırı Analizi

- Saldırı olduğunu nasıl anlarız?
 - Sistemimiz açılmıyordur, çalışmıyordur 😊
- Saldırı yapan bulunabilir mi?
- Saldırının tipini nasıl anlarız
 - Tcpdump, awk, sort, uniq
 - Ourmon anormallik tespit sistemi

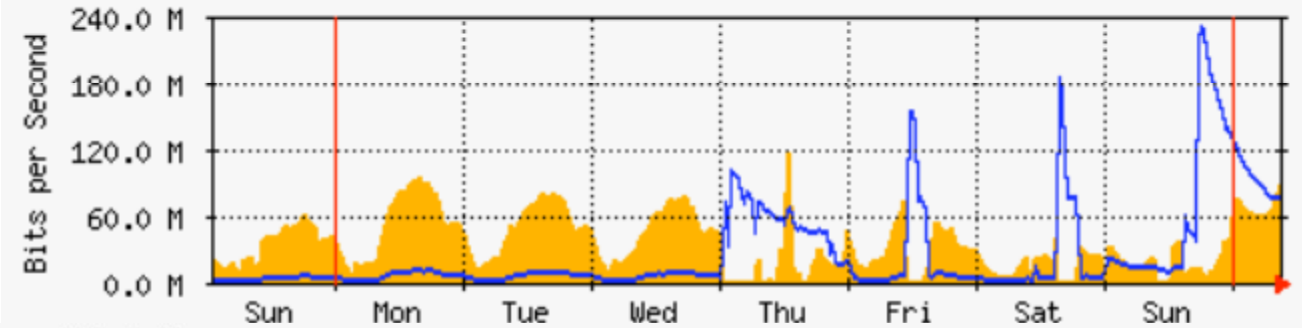


MRTG/RRD Grafikleri

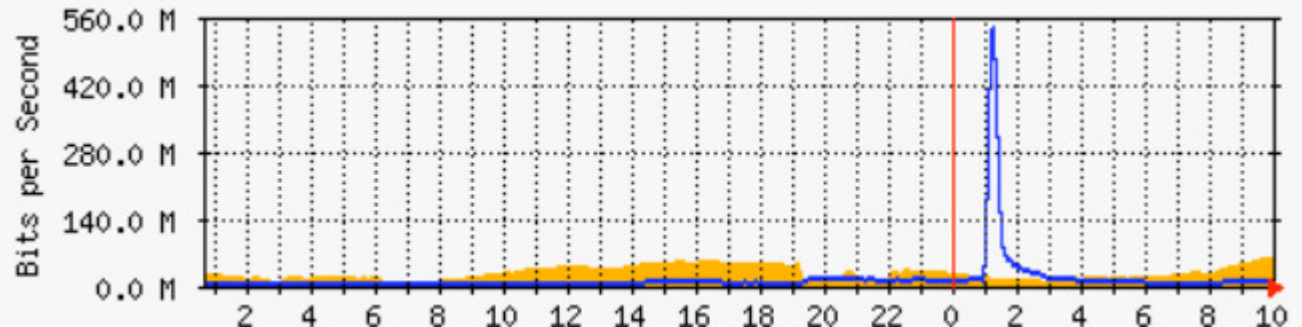
Normal Trafik



DDOS 1. Gün



DDOS 2.Gün



Synflood saldırıları

- Hedef sisteme spoof edilmiş milyonlarca ip adresinden SYN istekleri göndermek yoluyla kapasitesini zorlama*
- Eğer önlem alınmamışsa gelen her SYN bayraklı TCP paketine ACK+SYN dönülecek ve sistemde bu pakete ait bir oturum kaydı açılacaktır
- #hping -S -p 80 -flood ...
- *kaynaklar kısmında saldırı detaylarını anlatan dökümanlara referans verilmiştir



Synflood-Saldırısı

TD1-S-GuardLP-S-Guard12

```
all tcp 91.93.119.80:80 <- 103.131.182.240:7825 PROXY:SRC
all tcp 91.93.119.80:80 <- 171.65.240.206:7826 PROXY:SRC
all tcp 91.93.119.80:80 <- 5.127.195.153:7827 PROXY:SRC
all tcp 91.93.119.80:80 <- 122.32.90.157:7832 PROXY:SRC
all tcp 91.93.119.80:80 <- 119.235.224.104:7834 PROXY:SRC
all tcp 91.93.119.80:80 <- 90.53.137.38:7835 PROXY:SRC
all tcp 91.93.119.80:80 <- 151.72.104.214:7836 PROXY:SRC
all tcp 91.93.119.80:80 <- 242.238.66.155:7837 PROXY:SRC
all tcp 91.93.119.80:80 <- 198.184.103.225:7839 PROXY:SRC
all tcp 91.93.119.80:80 <- 100.46.236.244:7852 PROXY:SRC
all tcp 91.93.119.80:80 <- 10.214.62.175:7853 PROXY:SRC
all tcp 91.93.119.80:80 <- 201.157.91.214:7855 PROXY:SRC
all tcp 91.93.119.80:80 <- 42.227.66.52:7866 PROXY:SRC
all tcp 91.93.119.80:80 <- 153.32.137.174:7865 PROXY:SRC
all tcp 91.93.119.80:80 <- 18.32.105.174:7871 PROXY:SRC
all tcp 91.93.119.80:80 <- 77.144.77.31:7874 PROXY:SRC
all tcp 91.93.119.80:80 <- 184.214.103.212:7885 PROXY:SRC
all tcp 91.93.119.80:80 <- 137.72.246.179:7899 PROXY:SRC
all tcp 91.93.119.80:80 <- 145.77.221.93:7923 PROXY:SRC
all tcp 91.93.119.80:80 <- 252.246.145.147:7943 PROXY:SRC
all tcp 91.93.119.80:80 <- 17.227.214.127:7951 PROXY:SRC
all tcp 91.93.119.80:80 <- 195.201.235.71:7963 PROXY:SRC
all tcp 91.93.119.80:80 <- 246.131.161.108:7964 PROXY:SRC
all tcp 91.93.119.80:80 <- 69.103.66.64:7962 PROXY:SRC
all tcp 91.93.119.80:80 <- 147.113.208.224:7998 PROXY:SRC
all tcp 91.93.119.80:80 <- 176.37.242.86:8005 PROXY:SRC
all tcp 91.93.119.80:80 <- 5.170.144.101:8016 PROXY:SRC
all tcp 91.93.119.80:80 <- 221.46.142.198:8020 PROXY:SRC
all tcp 91.93.119.80:80 <- 171.221.177.238:8024 PROXY:SRC
all tcp 91.93.119.80:80 <- 96.167.100.86:8054 PROXY:SRC
all tcp 91.93.119.80:80 <- 93.9.140.95:8064 PROXY:SRC
all tcp 91.93.119.80:80 <- 125.69.182.98:8071 PROXY:SRC
all tcp 91.93.119.80:80 <- 208.252.5.195:8259 PROXY:SRC
all tcp 91.93.119.80:80 <- 123.176.127.227:8817 PROXY:SRC
all tcp 91.93.119.80:80 <- 199.214.94.155:8832 PROXY:SRC
all tcp 91.93.119.80:80 <- 95.77.55.120:8841 PROXY:SRC
all tcp 91.93.119.80:80 <- 241.144.65.196:8847 PROXY:SRC
all tcp 91.93.119.80:80 <- 5.147.214.7:8891 PROXY:SRC
all tcp 91.93.119.80:80 <- 7.86.41.144:8892 PROXY:SRC
all tcp 91.93.119.80:80 <- 123.131.252.134:8894 PROXY:SRC
all tcp 91.93.119.80:80 <- 46.175.131.246:8906 PROXY:SRC
all tcp 91.93.119.80:80 <- 214.147.236.230:9024 PROXY:SRC
```

```
[root@mail ~]# pfctl -si
No ALTQ support in kernel
ALTQ related functions disabled
Status: Enabled for 22 days 19:23:39          Debug: Urgent
```

State Table	Total	Rate
current entries	90497	
searches	365542015	185.5/s
inserts	18280637	9.3/s
removals	18190794	9.2/s
Counters		
match	44840624	22.8/s
bad-offset	0	0.0/s
fragment	3499	0.0/s
short	2	0.0/s
normalize	418	0.0/s
memory	0	0.0/s
bad-timestamp	0	0.0/s
congestion	0	0.0/s
ip-option	0	0.0/s
proto-cksum	1460	0.0/s
state-mismatch	64402	0.0/s
state-insert	5	0.0/s
state-limit	0	0.0/s
src-limit	55	0.0/s
synproxy	11319156	5.7/s

Syn Flood Engelleme

- Synflood engelleme standartı: Syncookie/SynProxy
- Linux sistemlerde Syncookie ile yapılabilir
 - Syncookie STATE tutmaz, state tablosunu kullanmaz
- OpenBSD PF Synproxy
 - En esnek çözüm: ip, port, paket özelliklerine göre aktif edebilme ya da kapatabilme özelliği
 - pass in log(all) quick on \$ext_if proto tcp to \$web_servers port {80 443} **flags S/SA synproxy state**
 - (((Loglama sıkıntı çıkarabilir)))



SynFlood Engelleme-II

- TCP timeout değerleriyle oynama
 - Default değerler yüksektir...
 - Saldırı anında dinamik olarak bu değerlerin 1/10'a düşürülmesi saldırı etkisini azaltacaktır.
- Linux için sysctl ile (manuel)
- OpenBSD PF için
 - set timeout {tcp.first 10, tcp.opening 10 tcp.closing 33, tcp.finwait 10, tcp.closed 20} gibi... Ya da
- Packet Filter adaptive timeout özelliği!
 - State tablosu dolmaya başladıkça timeout değerlerini otomatik azalt!



SynFlood engelleme-III

- Rate limiting(bir ip adresinden 500'den fazla istek geldiyse engellenecekler listesine ekle ve o ip adresine ait oturum tablosunu boşalt)
- OpenBSD Packet Filter
 - ... flags S/SA synproxy state (max-src-conn 500, max-src-conn-rate 100/1, overload <ddos_host> flush global)
- Linux iptables modülleri
 - -m limit vs



SynFlood engelleme-IV

- Beyaz liste, kara liste uygulaması
 - Daha önce state oluşturmuş, legal trafik geçirmiş ip adresleri
- Ülkelerin IP bloklarına göre erişim izni verme
 - Saldırı anında sadece Türkiye IP'lerine erişim açma
((IP spoofing kullanıldığı için çoğu zaman işe yaramaz)))
- DNS round-robin & TTL değerleriyle oynayarak engelleme



Linux Syncookie dezavantajları

- Donanım iyiye yeterli koruma sağlar
 - Syncookie CPU'ya yüklendiği için CPU %100'lere vurabilir
 - Ethernet kartının üreteceği IRQ'lar sistemi zora sokabilir
- Sadece kendisine syncookie koruması sağlar
- 1/0 . Aç - kapa özelliğindedir, çeşitli uygulamalarda SYNcookie sıkıntı çıkartabilir. Bir port/host için kapama özelliği yoktur



PF SynProxy Dezavantajları

- SynProxy=State=Ram gereksinimi
- State tablosu ciddi saldırılarda çok çabuk dolar
 - 100Mb~200.000 SYN=200.000 State
 - 40 saniyede 8.000.000 state = ~5GB ram ...
 - Tcp timeout değerlerini olabildiğince düşürmek bir çözüm olabilir
 - Timeout süresi 5 saniye olursa ?

(((Genel Çözüm: Stateless SynProxy çözümü)))



Rate limiting dezavantajları

- Akıllı saldırganın en sevdiği koruma yöntemidir😊
- Neden ?



ACK, FIN, PUSH Flood Saldırıları

- SynFlood'a karşı önlem alınan sistemlerde denenir.
- Hedef sisteme ACK, FIN, PUSH bayraklı TCP paketleri göndererek güvenlik cihazlarının kapasitesiniz zorlama
- Diğer saldırı tiplerine göre engellemesi oldukça kolaydır
- Etki düzeyi düşüktür



ACK,FIN,PUSH Saldırıları Engelleme

- Gelen ilk paketin SYN paketi olma zorunluluğu, oturum kurulmamış paketleri düşürme
- OpenBSD Packet Filter
 - scrub all
- Linux
 - iptables kurallar 😊



UDP Flood Saldırıları

- UDP stateless bir protokol, yönetimi zor!
- Paket boyutları küçük, etkisi yüksek
- Amaç UDP servislerini çökertmekten çok aradaki güvenlik cihazlarının kapasitesini zorlayıp cevap veremez hale getirmektir.
- Zaman zaman DNS sunuculara yönelik de yapılır
- Syncookie/synproxy gibi kolay bir çözümü yok!
 - Denenmiş, kanıtlanmış çözümü yok 😊



UDP Flood Engelleme

- UDP servisi yoksa Router üzerinden ACL ile komple protokolü engelleme
- Linux için
 - Udp timeout sürelerini kısaltma
 - Rate limiting kullanımı(spoofed ip kullanılmıyorsa)
- OpenBSD Packet Filter
 - UDP için state tutabilir(yalancı state)
 - Timeout değerleri kullanılarak udp sessionlarının çabucak kapatılması sağlanabilir
 - Probability özelliği kullanılabilir

((block in proto udp probability 50%)))



GET/POST Flood Saldırıları

- Synflood için önlem alınan yerlere karşı denenir
- Daha çok web sunucunun limitlerini zorlayarak sayfanın ulaşılamaz olmasını sağlar
- Önlemesi Synflood'a göre daha kolaydır
 - HTTP için IP spoofing “pratik olarak” imkansızdır.
- Rate limiting kullanılarak rahatlıkla önlenebilir
- False positive durumu
- #ab -n 100000 -c 5000 <http://www.google.com/>



1. **Introduction**
 2. **Background**
 3. **Methodology**
 4. **Results**
 5. **Discussion**
 6. **Conclusion**
 7. **References**
 8. **Appendix**
 9. **Index**
 10. **Table of Contents**
 11. **Abstract**
 12. **Summary**
 13. **Key Words**
 14. **Keywords**
 15. **Subject Headings**
 16. **Subject Headings**
 17. **Subject Headings**
 18. **Subject Headings**
 19. **Subject Headings**
 20. **Subject Headings**
 21. **Subject Headings**
 22. **Subject Headings**
 23. **Subject Headings**
 24. **Subject Headings**
 25. **Subject Headings**
 26. **Subject Headings**
 27. **Subject Headings**
 28. **Subject Headings**
 29. **Subject Headings**
 30. **Subject Headings**
 31. **Subject Headings**
 32. **Subject Headings**
 33. **Subject Headings**
 34. **Subject Headings**
 35. **Subject Headings**
 36. **Subject Headings**
 37. **Subject Headings**
 38. **Subject Headings**
 39. **Subject Headings**
 40. **Subject Headings**
 41. **Subject Headings**
 42. **Subject Headings**
 43. **Subject Headings**
 44. **Subject Headings**
 45. **Subject Headings**
 46. **Subject Headings**
 47. **Subject Headings**
 48. **Subject Headings**
 49. **Subject Headings**
 50. **Subject Headings**
 51. **Subject Headings**
 52. **Subject Headings**
 53. **Subject Headings**
 54. **Subject Headings**
 55. **Subject Headings**
 56. **Subject Headings**
 57. **Subject Headings**
 58. **Subject Headings**
 59. **Subject Headings**
 60. **Subject Headings**
 61. **Subject Headings**
 62. **Subject Headings**
 63. **Subject Headings**
 64. **Subject Headings**
 65. **Subject Headings**
 66. **Subject Headings**
 67. **Subject Headings**
 68. **Subject Headings**
 69. **Subject Headings**
 70. **Subject Headings**
 71. **Subject Headings**
 72. **Subject Headings**
 73. **Subject Headings**
 74. **Subject Headings**
 75. **Subject Headings**
 76. **Subject Headings**
 77. **Subject Headings**
 78. **Subject Headings**
 79. **Subject Headings**
 80. **Subject Headings**
 81. **Subject Headings**
 82. **Subject Headings**
 83. **Subject Headings**
 84. **Subject Headings**
 85. **Subject Headings**
 86. **Subject Headings**
 87. **Subject Headings**
 88. **Subject Headings**
 89. **Subject Headings**
 90. **Subject Headings**
 91. **Subject Headings**
 92. **Subject Headings**
 93. **Subject Headings**
 94. **Subject Headings**
 95. **Subject Headings**
 96. **Subject Headings**
 97. **Subject Headings**
 98. **Subject Headings**
 99. **Subject Headings**
 100. **Subject Headings**
 101. **Subject Headings**
 102. **Subject Headings**
 103. **Subject Headings**
 104. **Subject Headings**
 105. **Subject Headings**
 106. **Subject Headings**
 107. **Subject Headings**
 108. **Subject Headings**
 109. **Subject Headings**
 110. **Subject Headings**
 111. **Subject Headings**
 112. **Subject Headings**
 113. **Subject Headings**
 114. **Subject Headings**
 115. **Subject Headings**
 116. **Subject Headings**
 117. **Subject Headings**
 118. **Subject Headings**
 119. **Subject Headings**
 120. **Subject Headings**
 121. **Subject Headings**
 122. **Subject Headings**
 123. **Subject Headings**
 124. **Subject Headings**
 125. **Subject Headings**
 126. **Subject Headings**
 127. **Subject Headings**
 128. **Subject Headings**
 129. **Subject Headings**
 130. **Subject Headings**
 131. **Subject Headings**
 132. **Subject Headings**
 133. **Subject Headings**
 134. **Subject Headings**
 135. **Subject Headings**
 136. **Subject Headings**
 137. **Subject Headings**
 138. **Subject Headings**
 139. **Subject Headings**
 140. **Subject Headings**
 141. **Subject Headings**
 142. **Subject Headings**
 143. **Subject Headings**
 144. **Subject Headings**
 145. **Subject Headings**
 146. **Subject Headings**
 147. **Subject Headings**
 148. **Subject Headings**
 149. **Subject Headings**
 150. **Subject Headings**
 151. **Subject Headings**
 152. **Subject Headings**
 153. **Subject Headings**
 154. **Subject Headings**
 155. **Subject Headings**
 156. **Subject Headings**
 157. **Subject Headings**
 158. **Subject Headings**
 159. **Subject Headings**
 160. **Subject Headings**
 161. **Subject Headings**
 162. **Subject Headings**
 163. **Subject Headings**
 164. **Subject Headings**
 165. **Subject Headings**
 166. **Subject Headings**
 167. **Subject Headings**
 168. **Subject Headings**
 169. **Subject Headings**
 170. **Subject Headings**
 171. **Subject Headings**
 172. **Subject Headings**
 173. **Subject Headings**
 174. **Subject Headings**
 175. **Subject Headings**
 176. **Subject Headings**
 177. **Subject Headings**
 178. **Subject Headings**
 179. **Subject Headings**
 180. **Subject Headings**
 181. **Subject Headings**
 182. **Subject Headings**
 183. **Subject Headings**
 184. **Subject Headings**
 185. **Subject Headings**
 186. **Subject Headings**
 187. **Subject Headings**
 188. **Subject Headings**
 189. **Subject Headings**
 190. **Subject Headings**
 191. **Subject Headings**
 192. **Subject Headings**
 193. **Subject Headings**
 194. **Subject Headings**
 195. **Subject Headings**
 196. **Subject Headings**
 197. **Subject Headings**
 198. **Subject Headings**
 199. **Subject Headings**
 200. **Subject Headings**
 201. **Subject Headings**
 202. **Subject Headings**
 203. **Subject Headings**
 204. **Subject Headings**
 205. **Subject Headings**
 206. **Subject Headings**
 207. **Subject Headings**
 208. **Subject Headings**
 209. **Subject Headings**
 210. **Subject Headings**
 211. **Subject Headings**
 212. **Subject Headings**
 213. **Subject Headings**
 214. **Subject Headings**
 215. **Subject Headings**
 216. **Subject Headings**
 217. **Subject Headings**
 218. **Subject Headings**
 219. **Subject Headings**
 220. **Subject Headings**
 221. **Subject Headings**
 222. **Subject Headings**
 223. **Subject Headings**
 224. **Subject Headings**
 225. **Subject Headings**
 226. **Subject Headings**
 227. **Subject Headings**
 228. **Subject Headings**
 229. **Subject Headings**
 230. **Subject Headings**
 231. **Subject Headings**
 232. **Subject Headings**
 233. **Subject Headings**
 234. **Subject Headings**
 235. **Subject Headings**

Bilgi Güvenliği Akademisi
www.guvenlikegitimleri.com

HTTP Flood engelleme

- OpenBSD Packet Filter

pass in log(all) quick on \$ext_if proto tcp to
\$web_server port {80 443} flags S/SA synproxy state
(max-src-conn 1000, max-src-conn-rate 100/3,
overload <ddos_host> flush global)

table <ddos_host> persist file /etc/ddos

block in quick log on \$ext_if from <ddos_host>

- False positive durumuna karşı her saat başı yasaklı ip listesini sıfırla!
- Sayfa yoğunluğuna göre Kurallar düzenlenmeli

```
[root@netdos1 ~]# pfctl -t ddos_host -T show
No ALTQ support in kernel
ALTQ related functions disabled
193.108.1.120
194.105.87.2
212.105.25.12
212.177.127.24
You have new mail in /var/mail/root
```



HTTP Get Flood Engelleme-II

- Apache Loglarını inceleyen ve belirli bir değerin üzerinde istek gönderenleri iptables ile engelleyen bir script yazılabilir
- Netstat ile establish olmuş bağlantılardan belirli değerin üzerindeki engellenen script yazılabilir
- Apache dos engelleme modülleri kullanılabilir



Uygulama Seviyesi DOS Engelleme

- Bazı HTTP Flood saldırıları HTTP Keepalive kullanır
 - Bir TCP bağlantısı içerisinde yüzlerce HTTP isteği gönderme
- Firewall ile engellemek(Firewall sadece TCP seviyesinde müdahale ediyor paketlere)kolay değil
- Snort imzaları kullanılabilir, yazılabilir
 - Trafiğin içerisinde yakalanacak ortak bir değer(user-agent vs)

```
alert tcp any any -> any 80 (msg:"HTTP GET Flood Attack Attempt"; content:"GET";  
nocase; depth:10; detection_filter: track by_src, count 90, seconds 3; sid:1000001;  
rev:1;)
```



BotNet Engelleme

- Botnete üye olan makineler merkezden yönetilirler
- Merkez sistemleri engelleme çoğu zaman saldırıları azaltmada işe yarayacaktır ve sizin ağınızdan DDOS yapılmasını engelleyecektir.

Welcome to the Zeus Tracker

The Zeus Tracker tracks Zeus Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the [FAQ](#) or send me a email ([contact](#)).

Here are some quick statistics about the ZeusS crimeware:

- Zeus C&C servers tracked: **1334**
- Zeus C&C servers online: **727**
- Average binary Antivirus detection rate: **45.97%**

You can find more interesting statistics about the ZeusS crimeware on the [Zeus Tracker statistic page](#).
The map below shows a dot for each ZeusS Command&Control server (ip or domain).

Note: If you are using IE 6/7 you will get a security warning due to the fact that the Google maps API currently does not support SSL (https).



Ağınızdan DDOS Yapılmasını Engelleme

- DDOS saldırılarında belirleyici iki temel etken:
 - IP spoofing
 - Bir ip adresinden anormal seviyede trafik gönderimi
- IP spoofing engelleme(ağınızdan dışarı doğru)
 - URPF(Unicast Reverse Path Forwarding)
 - block in from urpf-failed to any (OpenBSD PF)
- Ip başına anormallik tespiti
 - Ourmon, Packet Filter rate limit
- Netflow/pfflowd



DDOS Testleri Gerçekleştirme

- Başkaları yapmadan siz kendi sistemlerinizi test edin
- Test için gerekli araçlar
 - Hping, nmap, nping, isic, ab çeşitli perl scriptleri
- Linux kurulu bir iki laptop ve Ggabit switch



DDOS Eğitimi

BİLGİ GÜVENLİĞİ AKADEMİSİ

WWW.GUVENLIKEGITIMLERI.COM

ANA SAYFA

EĞİTİMLER

EĞİTMENLER

MAKALELER

EĞİTİM NOTLARI

HAKKIMIZDA

KAYNAKLAR

DDOS Saldırı Tipleri

DDOS saldırıları Internet dünyasının en eski ve en etkili saldırılarından. DDOS saldırılarına karşı kesin bir reçete olamayacağı için bu tip saldırılarla karşı karşıya kalmadan konu hakkında detaylı bilgi sahibi olmak en büyük silahtır. Konu hakkında bilgi sahibi olmadan alınacak DDOS koruma ürünleri ayrı bir DOS'a(servis kesintisi) sebep olabilmektedir.

Bu eğitimle birlikte sık kullanılan ve etkili olan DDOS yöntemleri, çalışma mantıkları, uygulamaları ve korunma yöntemlerini hem teorik olarak öğrenme hem de pratik olarak görme fırsatı yakalayacaksınız. Eğitimciler Türkiye ve yurt dışında çeşitli firmaların DDOS Testlerini yapmış uzman kişilerden oluşmaktadır.

DDOS Saldırı Tipleri ve Engelleme Yöntemleri Eğitim İçeriği

<http://www.guvenlikegitimleri.com/new/egitimler/ddos-saldiri-tipleri>



Kaynaklar

- [SynFlood DDOS Saldırıları ve Korunma Yolları](#)
- [Web Sunuculara Yönelik DOS/DDOS Saldırıları](#)
- [<http://www.ankasec.org/arsiv/ankasec09/DOSDDOSAtaklariveKorunmaYontemleri.pdf>](#)
- OpenBSD PF FAQ
- Arbor Networks
- [<http://www.shadowserver.org/wiki/>](#)



Teşekkürler...

