DDoS Saldırı Analizi

DDoS Saldırılarında IP Analizi

Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>
http://www.bga.com.tr
6/10/2010

İçerik

Giriş

Çıktığı ilk günden itibaren popülaritesini hiç kaybetmemiş nadir tehditlerden biri DDoS saldırılarıdır. Bunun temel sebebi yaygın kullanılan DoS/DDoS saldırılarının protokollerin doğasındaki tasarım hatalarını kullanmasıdır. Günümüzde kullandığımız protokoller yenileriyle değiştirilmeden de bu saldırı tipinden %100 korunmak mümkün olmayacaktır.

DDoS saldırılarında dikkate alınması gereken iki temel husus vardır. İlki saldırıyı engelleme ikincisi saldırının kim tarafından ne şiddetde ve hangi yöntemler, araçlar kullanılarak yapıldığınının belirlenmesidir.

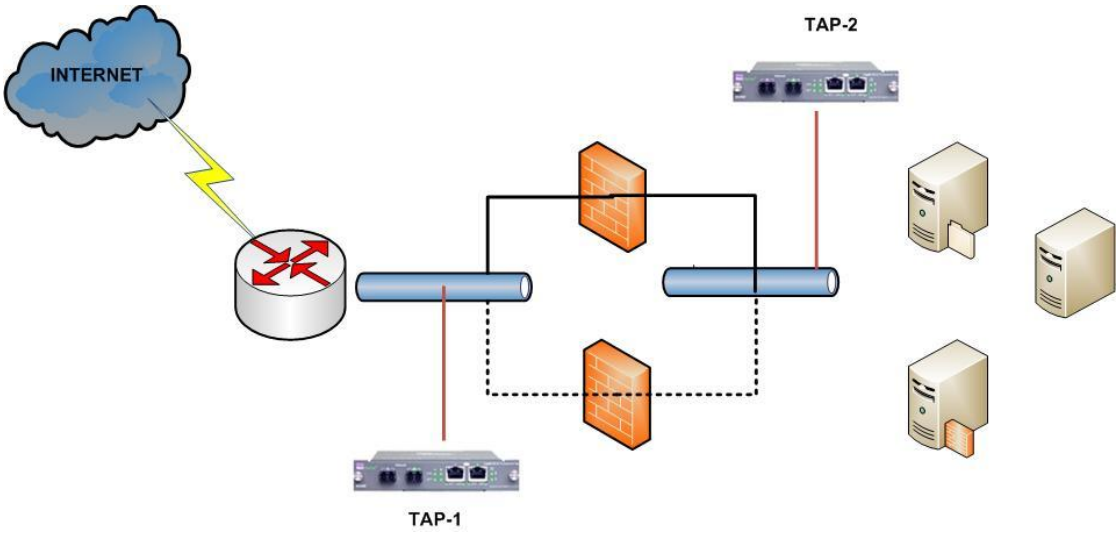
Genellikle saldırı engelleme kısmı dikkate alınmaktadır ve plansız bir şekilde DDoS saldırıları anlık olarak durdurulmaya çalışılmaktadır. Oysa yapılan araştırmalar göstermiştir ki bir kere DDoS saldırısına maruz kalıp yenilen bir kurum/sistem aynı yıl içerisinde defalarca DDoS saldırısına maruz kalmıştır.

Yapılması gereken hem saldırının acilen "planlı" bir şekilde durdurulması, engellenmesi hem de saldırı sonrası analiz için kullanılacak delillerin toplanmasıdır.

DDoS Analizi İçin Gerekli Yapının Kurulması

DDoS saldırısı esnasında çok basit işlemlerle toplanacak deliller saldırı sonrası analizlerde olduça yardımcı olacaktır. Saldırının hangi şiddette, hangi protokoller kullanılarak (TCP, UDP, ICMP, HTTP , SMTP vs) ne tip (packet flood, bandwithd aşırma) ve kimler (gerçek ip adresleri, spoof edilmiş ip adresleri, botnet kullanımı) tarafından gerçekleştirildiği vs.

DDoS Saldırılarında sağlıklı analiz yapabilmek için uygun yerlere TAP cihazları yerleştirilmelidir. Bu cihazlar aracılığıyla saldırı anında aktif sistemleri etkilemeden log toplama imkanı olacaktır.



Saldırı Analizinde Cevabı Aranan Sorular

Herhangi bir konuda analize başlamadan yapılması gereken ilk iş konuyla ilgili sorulabilecek soruları çıkarmak ve analizi bu sorulara göre planlamak olmalıdır. DDoS saldırı analizi yaparken aynı yöntemi uygulayarak sağlıklı sonuçlar elde edilebilir. Bu yazıda cevabını aradığımız sorular:

- Gerçekten bir DDoS saldırısı var mı?
- Varsa nasıl anlaşılır?
- DDoS saldırısının tipi nedir?
- DDoS saldırısının şiddeti nedir?
- Saldırı ne kadar sürmüş?
- DDoS saldırısında gerçek IP adresleri mi spoofed IPadresleri mi kullanılmış?
- DDoS saldırısı hangi ülke/ülkelerden geliyor?

Alet Çantasında Bulunması Gereken Araçlar

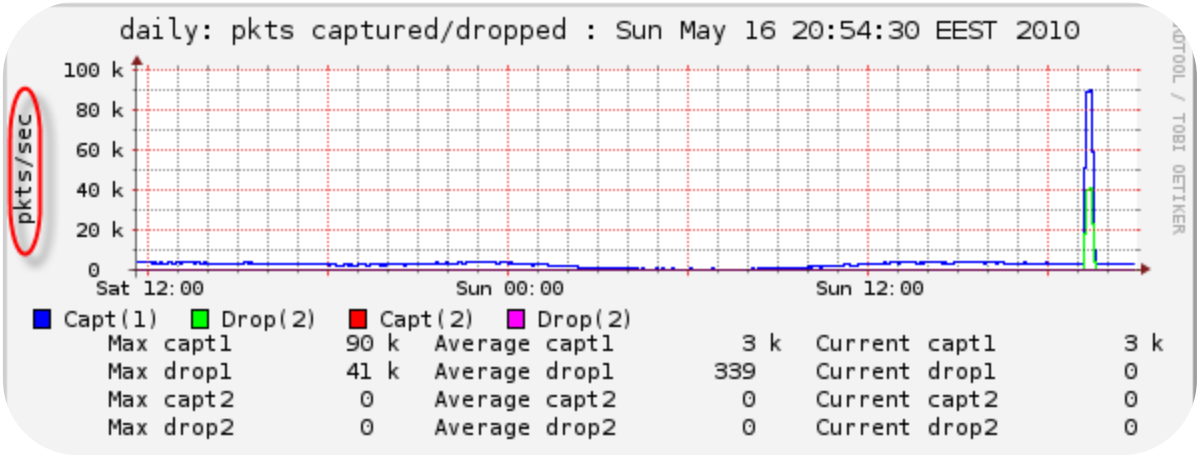
DDoS saldırı analizine başlamadan elimizin altında bulunması gereken çeşitli araçlar vardır. Bu yazıda DDoS analizi için kullanılan tüm araçlar internet üzerinden ücretsiz edinilebilecek açık kaynak kodlu yazılımlardır.

Tcpstat, tcpdstat, tcptrace tcpdump, ourmon, argus, urlsnarf, snort, aguri, cut, grep, awk, wc …

DDoS Saldırı Tespit Sistemleri

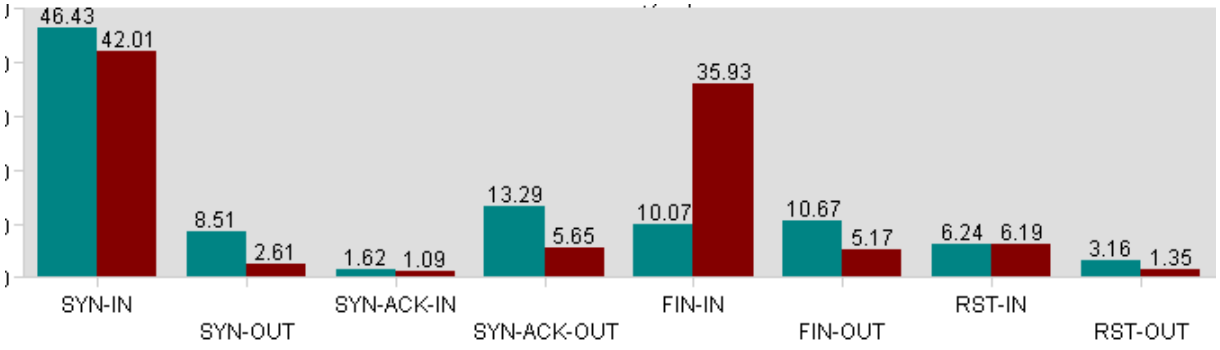
İhtiyacımız DDoS saldırılarını en kısa sürede belirlemek ve herhangi bir DDoS saldırısı esnasında saldırıya ait tüm paketleri loglayacak bir sistemdir. Internet üzerinden ücretsiz edinilebilecek açık kod ADS sistemi olan Ourmon, DDoS saldırılarını belirleme amaçlı kullanılabilir. Benzer şekilde tcpstat aracı da sistemdeki paket anormalliklerini tespit etmek ve saldırı anında otomatik paket kadyına başlamak için kullanılabilir.

Resim-2'de Ourmon arabiriminden alınan çıktıda net bir şekilde DDoS saldırısı gözükmektedir. Ortalama 10.000 ler seviyesinde seyreden PPS(Packet Per Second) değeri aniden 90.000ler seviyesine çıkmıştır.



Resim-2

Resim-3 McAfee Intrushield IPS sisteminin paket anormalliğini gösteren bileşeninden alınmıştır. Bu bileşen kullanılarak saldırılar rahatlıkla farkedilebilir.



Resim-3

DDoS Saldırılarında Delil Toplama

DDoS saldırılarında sonradan incelenmek üzere paketler kaydedilmelidir. Bunun için kaydedilen trafik miktarına bağlı olarak ciddi sistemlere(CPU, RAM, Disk alanı bakımından) ihtiyaç olabilir.

Dikkat edilmesi gereken en önemli husus paket kaydetme işleminin kesinlikle aktif cihazlar tarafından (IPS, DDoS engelleme Sistemi, Firewall) yapılmaması gerektiğidir. Bunun nedeni açıktır. DDoS esnasında aktif sistemler zaten normalin üzerinde bir yoğunluğa sahiptir ve gelen-giden paketleri kaydetmek için ek performansişlemci gücü bulamayabilir. Daha da kötüsü aktif sistemler paket kaydetmeye çalışırken asıl işlevi olan engelleme işlemini gerçekleştiremeyebilir.

Eğer DDoS saldırı engelleme sistemi kısa sürede saldırının tipini anlayabildiyse ve eğer saldırı uygulama seviyesi bir protocol kullanılarak gerçekleştirildiyse(HTTP GET Flood) sadece paket başlık bilgilerini kaydetmek yeterli olmayacaktır, tüm protocol bilgileri(+payload) kaydedilmesi gerekir.

Eğer saldırı SYN flood, ACK flood, UDP flood gibi sadece paket başlık bilgilerini kullanarak gerçekleştirilmişse payload bilgisinin kaydedilmesi gerekmeyecektir.

Paket Kaydetme

Paket kaydetme için Linux/FreeBSD üzerinde tcpdump en uygun seçenektir. 10 Gb ortamlarda klasik libpcap yerine alternative kütüphaneler tercih edilmelidir.

Tcpdump ile paket kaydetme

```
#tcpdump –n  -w ddostest1.pcap
```

Eğer payload bilgisi de gerekliyse tcpdump'a –s0 parametresi de eklenmelidir. Kayıt esnasında tek bir dosya değil de farklı farklı dosyalara kayıt yapılması istenirse –C parametresi incelenmelidir.

DDoS Saldırı Tipi Belirleme

DDoS saldırı tipini belirlemek için saldırı esnasında kaydedilen paket dosyalarını kullanılacaktır.

Saldırı tipi belirlemede ilk olarak hangi protokol ne kadar istek almış bilgisine ihtiyaç duyulur. Bu bilgi sonrasında DDoS saldırısının tipi hakkındaki ilk bilgi ortaya çıkacaktır.

Tcpdstat kullanılarak pcap dosyalarında(saldırı esnasındaki kayıt dosyaları) hangi protocol ne oranda kullanılmış bilgisi aşağıdaki gibi alınabilir.

```
# tcpdstat -n ddos.pcap

DumpFile:  ddos.pcap
FileSize: 45.58MB
Id: 201005181114
StartTime: Tue May 18 11:14:57 2010
EndTime:   Tue May 18 11:16:19 2010
TotalTime: 81.59 seconds
TotalCapSize: 37.38MB  CapLen: 96 bytes
# of packets: 537187 (170.55MB)
AvgRate: 17.55Mbps  stddev:7.87M

### Packet Size Distribution (including MAC headers) ###
<<<<
 [  32-  63]:    337610
 [  64-  127]:     13257
 [  128-  255]:     5341
 [  256-  511]:     19289
 [  512- 1023]:    104016
 [ 1024- 2047]:     57674
>>>>

### Protocol Breakdown ###
<<<<
    protocol         packets             bytes         bytes/pkt
------------------------------------------------------------------------------
[0] total         537187 (100.00%)      178836761 (100.00%)    332.91
[1] ip           537082 ( 99.98%)      178830375 (100.00%)    332.97
[2]  tcp          529590 ( 98.59%)      178126550 ( 99.60%)    336.35
[3]   http(s)      169318 ( 31.52%)      123244600 ( 68.91%)    727.89
[3]   http(c)      113553 ( 21.14%)       34132760 ( 19.09%)    300.59
[3]   squid          9 (  0.00%)           540 (  0.00%)     60.00
[3]   smtp         238109 ( 44.33%)       14288975 (  7.99%)     60.01
[3]   nntp           3 (  0.00%)           180 (  0.00%)     60.00
```

```
[3]   ftp          24 (  0.00%)          1510 (  0.00%)    62.92
[3]   pop3          6 (  0.00%)           360 (  0.00%)    60.00
[3]   imap          1 (  0.00%)            60 (  0.00%)    60.00
[3]   telnet        7 (  0.00%)           448 (  0.00%)    64.00
[3]   ssh           4 (  0.00%)           366 (  0.00%)    91.50
[3]   dns           4 (  0.00%)           240 (  0.00%)    60.00
[3]   bgp           4 (  0.00%)           240 (  0.00%)    60.00
[3]   napster       5 (  0.00%)           300 (  0.00%)    60.00
[3]   realaud       3 (  0.00%)           180 (  0.00%)    60.00
[3]   rtsp          7 (  0.00%)           420 (  0.00%)    60.00
[3]   icecast       5 (  0.00%)           300 (  0.00%)    60.00
[3]   hotline       3 (  0.00%)           180 (  0.00%)    60.00
[3]   other      8525 (  1.59%)       6454891 (  3.61%)   757.17
[2]  udp         7478 (  1.39%)        702824 (  0.39%)    93.99
[3]   dns         268 (  0.05%)         32774 (  0.02%)   122.29
[3]   other      7210 (  1.34%)        670050 (  0.37%)    92.93
[2]  icmp          14 (  0.00%)          1001 (  0.00%)    71.50
[1] ip6             1 (  0.00%)           146 (  0.00%)   146.00
[2]  udp6           1 (  0.00%)           146 (  0.00%)   146.00
[3]   other         1 (  0.00%)           146 (  0.00%)   146.00
>>>>
```

Çıktıda dikkatimizi aşağıdaki satırlar çekmekte.

```
[2]  tcp        529590 ( 98.59%)      178126550 ( 99.60%)   336.35
[3]   smtp      238109 ( 44.33%)       14288975 (  7.99%)    60.01
```

Bu satırlara bakarak şu yorum yapılabilir: Saldırı TCP kullanılarak gerçekleştirilmiş ve hedef port SMTP'dir.

Eğer çıktı aşağıdaki gibi olsaydı: (%99 oranında UDP) rahatlıkla saldırının TCP tabanlı değil UDP tabanlı olduğu yorumu yapılabilirdi.

```
# tcpdstat -n ddos1.pcap

DumpFile:  ddos1.pcap
FileSize: 0.36MB
Id: 201005181127
StartTime: Tue May 18 11:27:53 2010
EndTime:   Tue May 18 11:28:20 2010
TotalTime: 27.78 seconds
TotalCapSize: 0.30MB  CapLen: 96 bytes
# of packets: 3464 (320.10KB)
AvgRate: 91.67Kbps  stddev:50.34K
```

```
### Packet Size Distribution (including MAC headers) ###
<<<<
[  64-  127]:     3362
[ 128-  255]:       89
[ 256-  511]:       13
>>>>


### Protocol Breakdown ###
<<<<
    protocol         packets             bytes         bytes/pkt
--------------------------------------------------------------------------
[0] total          3464 (100.00%)        327782 (100.00%)    94.63
[1] ip             3462 ( 99.94%)        327490 ( 99.91%)    94.60
[2] udp            3462 ( 99.94%)        327490 ( 99.91%)    94.60
[3]   dns           106 (  3.06%)         12378 (  3.78%)    116.77
[3]   other        3356 ( 96.88%)        315112 ( 96.13%)    93.90
[1] ip6               2 (  0.06%)           292 (  0.09%)    146.00
[2] udp6              2 (  0.06%)           292 (  0.09%)    146.00
[3]   other           2 (  0.06%)           292 (  0.09%)    146.00
```

Saldırının hangi protocol(TCP/UDP/ICMP) kullanılarak gerçekleştiği bilgisi elde edildikten sonraki aşama gerçekte hangi saldırı yönteminin kullanıldığını bulmak olacaktır. Eğer UDP flood ise doğrudan kaynak IP adresi inceleme gerçekleştirilebilir fakat TCP kullanıldıysa işin seyri biraz değişecektir.

TCP kullanılarak gerçekleştirilen DDoS saldırı çeşitlerinden en sık tercih edilen ikili SYN Flood ve HTTP GET flood'dur.

TCP Bayrakları Kullanılarak Gerçekleştirilen DDoS Saldırıları

SYN Flood Saldırısı Analizi

Tcpdump aracının özellikleri kullanılarak trafik içerisinde sadece SYN bayrağı taşıyan paketler ayıklanabilir.

Sadece SYN bayraklı paketleri yakalama

```
# tcpdump –r ddos.pcap -n 'tcp[tcpflags] & tcp-syn == tcp-syn'
22:04:22.809998 IP 91.3.119.80.59204 > 11.22.33.44.53: Flags [S], seq 2861145144, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:22.863997 IP 91.3.119.80.59135 > 82.8.86.175.25: Flags [S], seq 539301671, win 65535, options
```

```
[mss 1460,sackOK,eol], length 0
22:04:22.864007 IP 91.3.119.80.59205 > 11.22.33.44.53: Flags [S], seq 4202405882, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:23.033997 IP 91.3.119.80.64170 > 11.22.33.44.53: Flags [S], seq 1040357906, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:23.146001 IP 91.3.119.80.59170 > 11.22.33.44.53: Flags [S], seq 3560482792, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:23.164997 IP 91.3.119.80.59171 > 20.17.222.88.25: Flags [S], seq 1663706635, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:23.384994 IP 91.3.119.80.59136 > 11.22.33.44.53: Flags [S], seq 192522881, win 65535, options
[mss 1460,sackOK,eol], length 0
22:04:23.432994 IP 91.3.119.80.59137 > 11.22.33.44.53: Flags [S], seq 914731000, win 65535, options
[mss 1460,sackOK,eol], length 0
```

ya da aynı işi yapan 'tcp[13] & 2 != 0' parametresi kullanılabilir.

Eğer saldırı klasik syn flood değilse alternatif flagleri deneyerek benzer sonuçlar elde edilebilir .

ACK Flood Analizi

Tcpdump kullanarak ACK bayraklı paketleri ayıklama

```
# tcpdump -i bce1 -n 'tcp[13] & 16 != 0'
```

FIN Flood Analizi

Tcpdump kullanarak FIN bayraklı paketleri ayıklama

```
# tcpdump -i bce1 -n 'tcp[13] & 1 != 0' and tcp port 80
```

tcp[13] demek TCP başlığındaki 13. byte anlamına gelir. Bu da bayrakları temsil eden byte'dır. Her bayrak için verilecek değer aşağıdaki resimden alınabilir.

SYN	ACK	FIN	RST	PUSH	URG	SYN+ACK
2	16	1	4	8	32	2+16=18

HTTP GET Flood Saldırısı

TCP paketleri içerisindeki GET komutlarının tcpdump ile ayıklanabilmesi için kullanılması gereken parametreler.

#tcpdump -n -r ddos3.pcap tcp port 80 and \(tcp[20:2] = 18225 \)

Saldırının Şiddetini Belirleme

DDoS saldırı analizine başlarken cevaplamaya çalıştığımız sorulardan biri de saldırının şiddetiydi. Saldırının şiddetini iki şekilde tanımlayabiliriz

1. Gelen trafiğin ne kadar bant genişliği harcadığı
2. Gelen trafiğin PPS değeri

Tcpstat aracı kullanılarak trafik dosyaları üzerinde saldırının PPS değeri, ne kadar bantgenişliği harcandığı bilgileri detaylı olarak belirlenebilir.

```
# tcpstat –r ddos_analizi.pcap  -o "Byte/s:%B MinPacketSize:%m  PPS:%p  TCP:%T   UDP:%U \n"  5
Byte/s:3401176.20 MinPacketSize:40  PPS:5929.20  TCP:29004   UDP:637
Byte/s:3145824.60 MinPacketSize:40  PPS:5247.60  TCP:25797   UDP:436
Byte/s:3140760.20 MinPacketSize:40  PPS:5252.40  TCP:25661   UDP:594
Byte/s:3850993.20 MinPacketSize:40  PPS:13602.80  TCP:66808   UDP:756
Byte/s:4360434.30 MinPacketSize:40  PPS:14904.80  TCP:73681   UDP:435
Byte/s:4460434.40 MinPacketSize:40  PPS:14874.80  TCP:73681   UDP:457
Byte/s:4960434.60 MinPacketSize:40  PPS:13904.80  TCP:73681   UDP:535
Byte/s:5460434.20 MinPacketSize:40  PPS:24904.80  TCP:73681   UDP:456
```

Saldırı Kaynağını Belirleme

DDoS saldırılarında en önemli sorunlardan biri saldırıyı gerçekleştiren asıl kaynağın bulunamamasıdır. Bunun temel sebepleri saldırıyı gerçekleştirenlerin zombie sistemler kullanarak kendilerini saklamaları ve bazı saldırı tiplerinde gerçek IP adresleri yerine spoof edilmiş IP adreslerinin kullanılmasıdır.

Saldırı analizinde saldırıda kullanılan IP adreslerinin gerçek IP'ler mi yoksa spoofed IPler mi olduğu rahatlıkla anlaşılabilir.

Internet üzerinde sık kullanılan DDoS araçları incelendiğinde IP spoofing seçeneği aktif kullanılırsa random üretilmiş sahte IP adreslerinden tek bir paket gönderildiği görülecektir. Yani saldırı sırasında kaydedilen dosya incelendiğinde fazla sayıda tek bağlantı gözüküyorsa saldırının spoof edilmiş IP adresleri kullanılarak gerçekleştirildiği hükmüne varılabilir.

Tek cümleyle özetleyecek olursak: **Eğer aynı IPden birden fazla bağlantı yoksa spoofed IP kullanılmış olma ihtimali yüksektir.**

```
#tcpdump -n -r ddos.pcap |awk -F" " '{print $3}'|cut -f1,2,3,4 -d"."|sort -n|uniq -c
   1 6.65.194.168
   1 6.65.208.248
   1 6.65.226.233
   1 6.65.232.125
   1 6.65.235.140
   1 6.65.248.199
   1 6.65.249.104
   1 6.65.32.97
   1 6.65.44.199
   1 6.65.48.49
   1 6.65.62.221
   1 6.65.62.30
   1 37.83.136.81
   1 37.83.14.12
   1 37.83.152.203
   1 37.83.164.223
   1 37.83.165.146
   1 37.83.166.132
   1 37.83.185.89
   1 37.83.194.21
   1 62.185.46.86
   1 62.185.60.100
   1 62.185.64.248
   1 62.185.66.32
   1 62.185.75.23
   1 62.185.9.193
   1 62.185.92.77
   1 62.185.96.16
```

Yukarıdaki tcpdump komutu saldırı yapan IP adreslerini ve ilgili IP adresinden saldırı boyunca kaç adet paket gönderildiğini bulmaya yarar. Çıktıdan da görüleceği üzere yoğun şekilde spoofed IP kullanılmıştır.

Saldırıda Kullanılan Top 10 IP Adresi

Saldırıda kullanılan ve en fazla paket gönderen 10 ip adresine ulaşılmak istenirse aşağıdaki komut satırı iş görecektir.

```
# tcpdump -r TEST.pcap -n |cut -f3 -d" "|cut -f1-4 -d"."|sort -n|uniq -c|awk -F" " '{print $2 "\t" $1 }'|sort -rn -k 2|head -10
reading from file TEST.pcap, link-type EN10MB (Ethernet)
11.22.228.246  482196
11.22.243.10   62095
11.22.228.73   27515
11.22.241.138  24972
93.18.207.182  24761
11.22.28.78   13205
195.142.247.7   5041
18.89.192.37   4870
78.16.195.145  4268
78.86.3.178   4157
```

Çıktıda sol taraf IP adresi, sağ taraf ise ilgili IP adresinden saldırı boyunca kaç adet paket gönderildiğidir.

HTTP GET Flood Saldırısında Kullanılan IP Adresleri

HTTP GET flood saldırılarında IP spoofing yapmak mümkün değildir. Bir system HTTP isteği gönderebilmesi için öncelikli olarak 3lü el sıkışmasını tamamlaması gerekmektedir. Günümüz işletim sistemi/ağ/güvenlik cihazlarında 3'lü el sıkışma esnasında TCP protokolünü kandırarak IP spoofing yapmak mümkün gözükmemektedir. Dolayısıyla HTTP GET flood saldırıları analizinde saldırı yapan IP adresleri %99 gerçek IP adreslerdir.

```
# tcpdump -n  -r ddos3.pcap  tcp port 80 and \( tcp[20:2] = 18225  \)|sort -k3 -n|cut -f3 -d" "|cut -f1,2,3,4 -d"."|sort -n |uniq -c
reading from file ddos3.pcap, link-type EN10MB (Ethernet)
 1092 62.202.27.120
  92 62.111.223.1
   7 62.227.26.27
52000 62.227.33.111
```

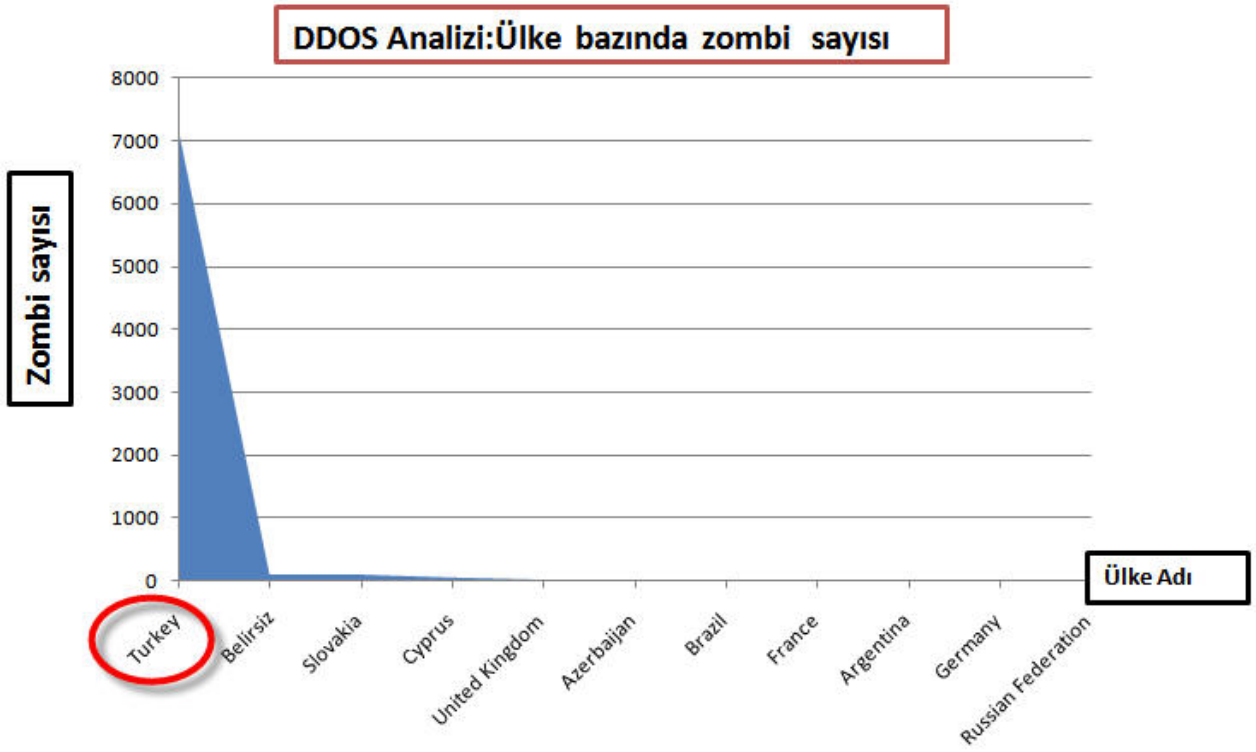
```
 63 62.72.23.102
 1300 66.229.63.26
  2 67.193.112.72
  1 77.77.31.226
31020 77.160.72.77
 93 77.161.12.233
 71 77.161.227.192
 90232 77.161.32.210
 23 77.162.1.137
  2 77.162.3.170
12900 77.162.76.177
 21 77.163.6.127
  3 77.163.132.37
 79100 77.163.217.137
 21 77.165.97.107
  9 77.166.197.232
 2700 77.166.60.175
 35100 77.166.65.133
 74200 77.167.126.119
 22009 77.169.152.239
 11891 77.171.175.77
…
…
```

Sağ taraf IP adresi, sol taraftaki sayı da ilgili IP adresinden kaç adet HTTP GET Flood isteği gönderildiğidir.

Saldırıda Kullanılan IP Adresleri Hangi Ülkeden?

Gerçekleştirilen saldırı bir botnet aracılığıyla gerçekleştirilmiş ve IP adresleri spoof edilmemişse saldırıda kullanılan IP adreslerinin hangi ülkelere ait olduğu bulunabilir.

Çıkan sonuç grafiğe döküldüğünde aşağıdakı çıktı alınacaktır.



Saldırı Paketlerini Pasif Snort Sisteminden Geçirme

Snort açık kaynak kodlu bir IPS sistemidir ve bünyesinde barndırdığı saldırı imzalarıyla çoğu klasik DDoS aracını /tipini tanmaktadır. Saldırı esnasında kaydedilen paketler Snort'un pasif IPS motorundan geçirilirse hangi saldırı tipleri/araçları kullanılmış bilgisi alınabilir.

#snort -r pids.pcap -c /usr/local/etc/snort/snort.conf -q –O

Jun 9 12:15:37 netdos1 snort: [1:2000545:6] ET SCAN NMAP -f -sS [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 0.0.0.0:45295 -> 0.0.0.0:80

Jun 9 12:15:37 netdos1 snort: [1:2000545:6] ET SCAN NMAP -f -sS [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 0.0.0.0:45296 -> 0.0.0.0:707

Jun 9 12:15:40 netdos1 snort: [1:408:5] ICMP Echo Request Flood [Classification: Misc activity] [Priority: 3]: {ICMP} 0.0.0.0 -> 0.0.0.0

Jun 1 10:15:23 netdos1 snort: [1:1000003:6] SYN Flood [Classification: DDoS] [Priority: 3]: {TCP} 0.0.0.0:1024 -> 0.0.0.0:80

Jun 9 12:15:37 netdos1 snort: [1:1000002:6] HTTP GET FlOOD [Classification: DDoS] [Priority: 2]: {TCP} 0.0.0.0:15295 -> 0.0.0.0:80