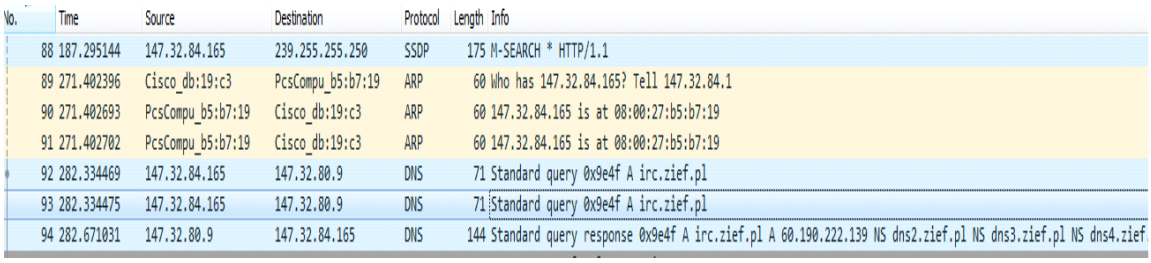
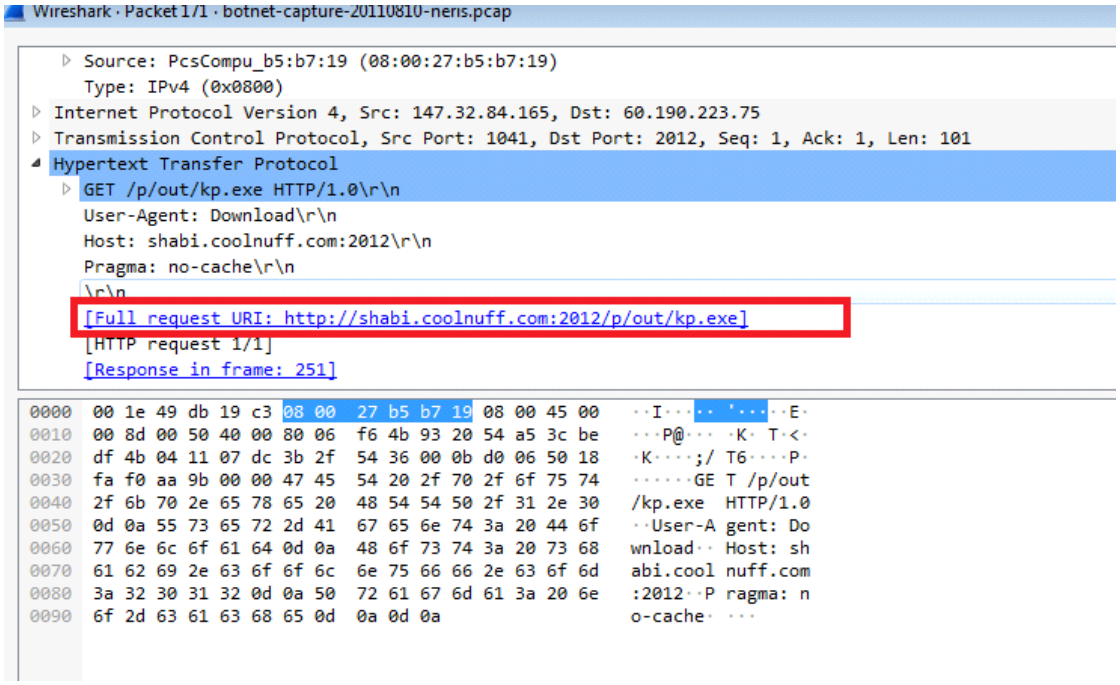
CTU-CAPTURE-BOTNET-42 Pcap Dosya Analizi

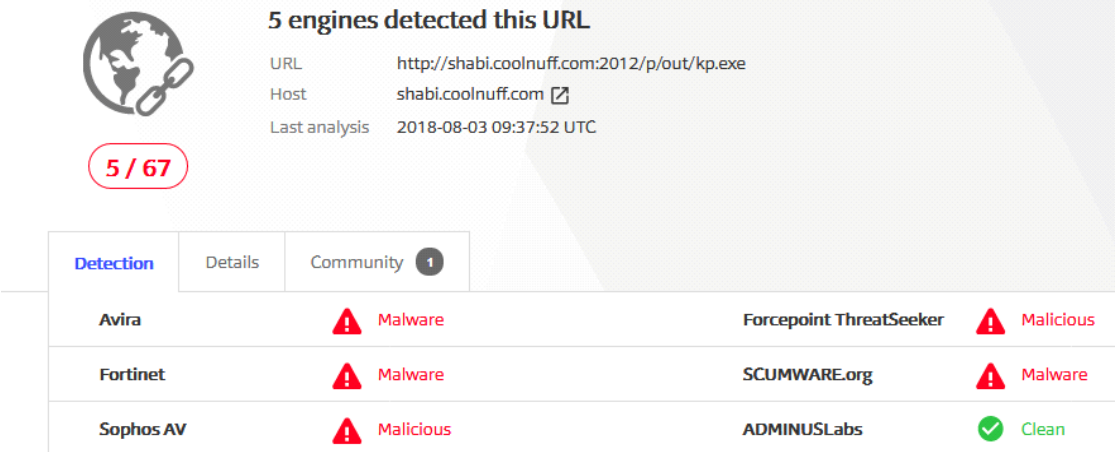
Pcap dosyasının içeriğine baktığımda paketlerin büyük bir kısmının 147.32.84.165 IP adresinden geldiğini farkettim. Bundan dolayı bu IP adresi tehlikeli olabilir düşüncesiyle çeşitli filtreler kullanarak devam edelim.



No.	Time	Source	Destination	Protocol	Length	Info
88	187.295144	147.32.84.165	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
89	271.402396	Cisco_db:19:c3	PcsCompu_b5:b7:19	ARP	60	Who has 147.32.84.165? Tell 147.32.84.1
90	271.402693	PcsCompu_b5:b7:19	Cisco_db:19:c3	ARP	60	147.32.84.165 is at 08:00:27:b5:b7:19
91	271.402702	PcsCompu_b5:b7:19	Cisco_db:19:c3	ARP	60	147.32.84.165 is at 08:00:27:b5:b7:19
92	282.334469	147.32.84.165	147.32.80.9	DNS	71	Standard query 0x9e4f A irc.zief.pl
93	282.334475	147.32.84.165	147.32.80.9	DNS	71	Standard query 0x9e4f A irc.zief.pl
94	282.671031	147.32.80.9	147.32.84.165	DNS	144	Standard query response 0x9e4f A irc.zief.pl A 60.190.222.139 NS dns2.zief.pl NS dns3.zief.pl NS dns4.zief



Tehlikeli olarak belirlediğim IP adresi yukarıda belirttiğim domain adresine GET isteğinde bulunarak bir exe dosyası çekmek istemiş. Bu URI'yi VirusTotal'de tarattığımda zararlı olduğunu gördüm.



Burada aklıma gelen bir başka çıkarım, istek yapılan sitelerin reklam,pop-up tarzında çıkabileceği oldu. Bunun sebebini ise tam olarak emin olamasamda istek yapılan sitelerden exe dışında GIF,JPEG gibi bağlantıların isteklerde olduğunu gördüğümden dolayı böyle bir tahmin yapabildim.

Dikkatimi çeken bir diğer durum ise http paketlerini incelediğimde sürekli olarak bir takım paketlerden sonra bot makinadan bir adrese POST isteği gönderdiğini farkettim. Bunun C&C ile olan iletişimi için kullanılabilir olduğunu düşünüyorum.

```
Hypertext Transfer Protocol
  POST /snapbn/gate.php HTTP/1.0\r\n
    [Expert Info (Chat/Sequence): POST /snapbn/gate.php HTTP/1.0\r\n]
      [POST /snapbn/gate.php HTTP/1.0\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: POST
    Request URI: /snapbn/gate.php
    Request Version: HTTP/1.0
  Host: finalcortex.com\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  Content-Length: 62\r\n
  \r\n
  [Full request URI: http://finalcortex.com/snapbn/gate.php]
```

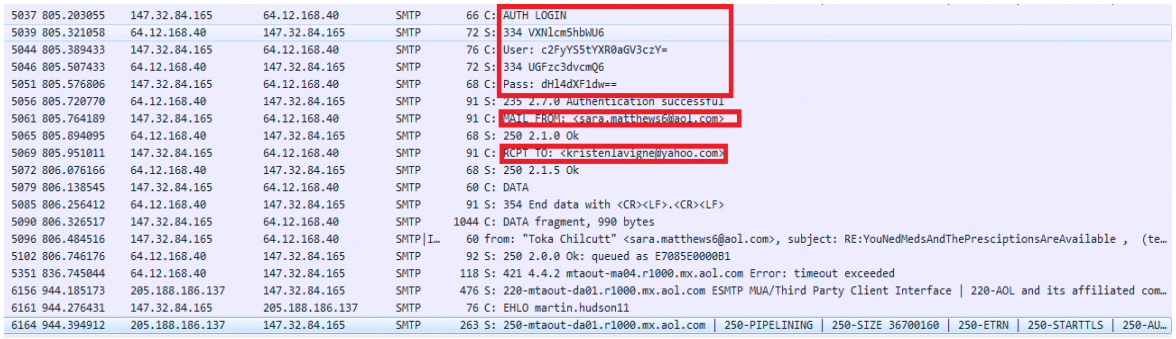
```
POST /snapbn/gate.php HTTP/1.0
Host: finalcortex.com
Keep-Alive: 300
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

id=SARUMAN_610d402662842e9f&version=1337&os=2600&s5=6906&done=HTTP/1.1 200 OK
Date: Wed, 10 Aug 2011 09:23:03 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Content-Length: 3
Connection: close
Content-Type: text/plain; charset=UTF-8

120
```

Bu yorumu yaptıktan sonra otomatik olarak söyleyebileceğim tahmin ise başta belirleyemediğim C&C ile iletişimin IRC ile değil HTTP ile yapılıyor olabileceği oldu.

Botnet karakteristiklerini araştırdığımda spam mail amacıyla kullanıldıklarını görünce birde SMTP filtresi uygulamak istedim. Bot makinanın farklı mail adreslerine mail gönderdiğini tespit ettim.

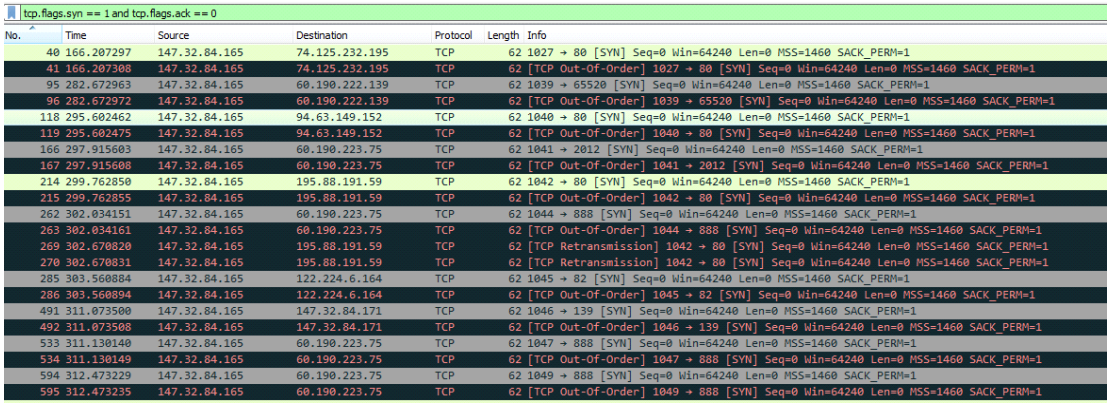


Yukarıdaki örnek bir spam maili. @aol.com uzantısından farklı mail adreslerine spam mail gönderiliyor.

Botnet'in diğer bir karakteristiği olan servis dışı bırakma saldırısını incelemek için uyguladığım

filtre " tcp.flags.syn == 1 and tcp.flags.ack == 0"(yaklaşık 65 bin paket yakalandı, toplam paketlerin %20'sini oluşturuyor.)

! Anormal Trafik



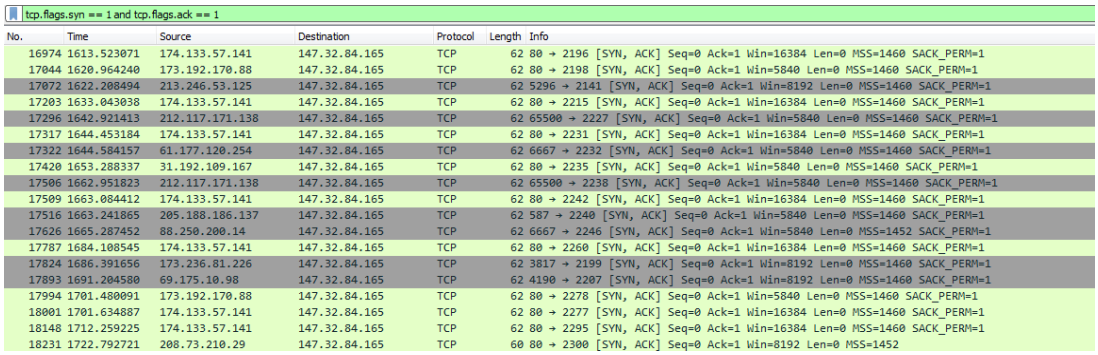
tcp.flags.syn == 1 and tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
40	166.207297	147.32.84.165	74.125.232.195	TCP	62	1027 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
41	166.207308	147.32.84.165	74.125.232.195	TCP	62	[TCP Out-Of-Order] 1027 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
95	282.672963	147.32.84.165	60.190.222.139	TCP	62	1039 → 65520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
96	282.672972	147.32.84.165	60.190.222.139	TCP	62	[TCP Out-Of-Order] 1039 → 65520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
118	295.602462	147.32.84.165	94.63.149.152	TCP	62	1040 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
119	295.602475	147.32.84.165	94.63.149.152	TCP	62	[TCP Out-Of-Order] 1040 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
166	297.915603	147.32.84.165	60.190.223.75	TCP	62	1041 → 2012 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
167	297.915608	147.32.84.165	60.190.223.75	TCP	62	[TCP Out-Of-Order] 1041 → 2012 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
214	299.762850	147.32.84.165	195.88.191.59	TCP	62	1042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
215	299.762855	147.32.84.165	195.88.191.59	TCP	62	[TCP Out-Of-Order] 1042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
262	302.034151	147.32.84.165	60.190.223.75	TCP	62	1044 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
263	302.034161	147.32.84.165	60.190.223.75	TCP	62	[TCP Out-Of-Order] 1044 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
269	302.670820	147.32.84.165	195.88.191.59	TCP	62	[TCP Retransmission] 1042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
270	302.670831	147.32.84.165	195.88.191.59	TCP	62	[TCP Retransmission] 1042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
285	303.560884	147.32.84.165	122.224.6.164	TCP	62	1045 → 82 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
286	303.560894	147.32.84.165	122.224.6.164	TCP	62	[TCP Out-Of-Order] 1045 → 82 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
491	311.073500	147.32.84.165	147.32.84.171	TCP	62	1046 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
492	311.073508	147.32.84.165	147.32.84.171	TCP	62	[TCP Out-Of-Order] 1046 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
533	311.130140	147.32.84.165	60.190.223.75	TCP	62	1047 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
534	311.130149	147.32.84.165	60.190.223.75	TCP	62	[TCP Out-Of-Order] 1047 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
594	312.473229	147.32.84.165	60.190.223.75	TCP	62	1049 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
595	312.473235	147.32.84.165	60.190.223.75	TCP	62	[TCP Out-Of-Order] 1049 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

Packets: 323154 · Displayed: 65467 (20.3%)

Burada amacım SYN flood saldırısı kullanılarak bir saldırı yapılmış mı onu görmekti. Bu tip saldırının yapıldığından emin olmak için bir diğer kullandığım filtre "tcp.flags.syn == 1 and tcp.flags.ack == 1" (yaklasık 2 bin paket yakalandı, toplam paketlerin %0.6 sını oluşturuyor)

!Normal Trafik

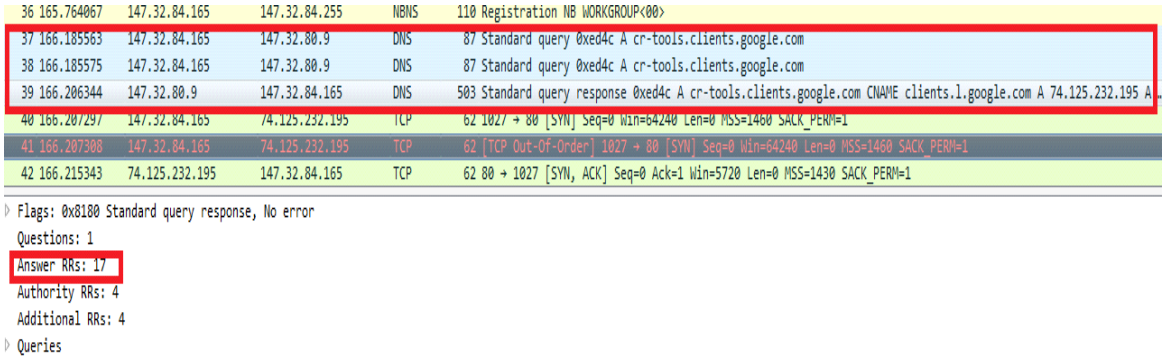


tcp.flags.syn == 1 and tcp.flags.ack == 1

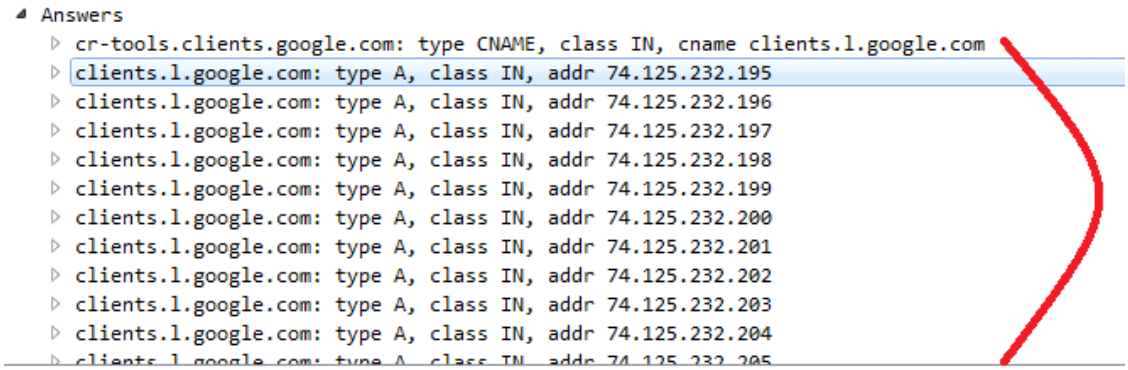
No.	Time	Source	Destination	Protocol	Length	Info
16974	1613.523071	174.133.57.141	147.32.84.165	TCP	62	80 → 2196 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17044	1620.964240	173.192.170.88	147.32.84.165	TCP	62	80 → 2198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17072	1622.208494	213.246.53.125	147.32.84.165	TCP	62	5296 → 2141 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
17203	1633.043038	174.133.57.141	147.32.84.165	TCP	62	80 → 2215 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17296	1642.921413	212.117.171.138	147.32.84.165	TCP	62	65500 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17317	1644.453184	174.133.57.141	147.32.84.165	TCP	62	80 → 2231 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17322	1644.584157	61.177.120.254	147.32.84.165	TCP	62	6667 → 2232 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17420	1653.288337	31.192.109.167	147.32.84.165	TCP	62	80 → 2235 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17506	1662.951823	212.117.171.138	147.32.84.165	TCP	62	65500 → 2238 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17509	1663.084412	174.133.57.141	147.32.84.165	TCP	62	80 → 2242 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17516	1663.241865	205.188.186.137	147.32.84.165	TCP	62	587 → 2240 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17626	1665.287452	88.250.200.14	147.32.84.165	TCP	62	6667 → 2246 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
17787	1684.108545	174.133.57.141	147.32.84.165	TCP	62	80 → 2260 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
17824	1686.391656	173.236.81.226	147.32.84.165	TCP	62	3817 → 2199 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
17893	1691.204580	69.175.10.98	147.32.84.165	TCP	62	4190 → 2207 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
17994	1701.480091	173.192.170.88	147.32.84.165	TCP	62	80 → 2278 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18001	1701.634887	174.133.57.141	147.32.84.165	TCP	62	80 → 2277 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
18148	1712.259225	174.133.57.141	147.32.84.165	TCP	62	80 → 2295 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1
18231	1722.792721	208.73.210.29	147.32.84.165	TCP	60	80 → 2300 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452

Packets: 323154 · Displayed: 1871 (0.6%)

ACK bayrağı set edilen paketlerin sayısı, set edilmeyen paketlerin sayısından az ise bir servis dışı bırakma saldırısı yapıldığı muhtemeldir.

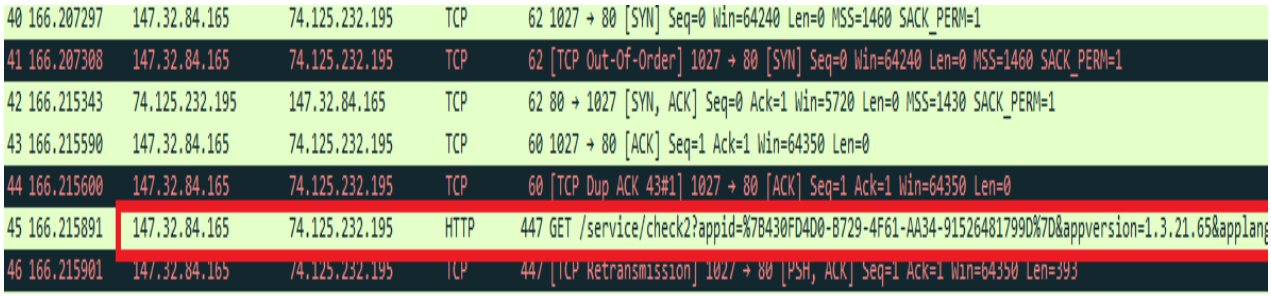


İlk yakalanan paketlere baktığımda infected makinenin clients.l.google.com CNAME 'ine sahip adrese sorgu attığını gördüm. Bu sorgu sonucunda geri dönen resource records sayısı ise 17.



Ve cevapta dönen adresler burada. Bu adreslerin fazla sayıda olması anormal bir durum olarak değerlendirilmelidir. Çünkü genellikle bu adresler bir C&C sunucusa ait olabilir. Ve bir önceki ekran görüntüsüne tekrar bakıldığında 47.125.232.195 adresine bir TCP bağlantısı isteği başlatılıyor ve iletişim kuruluyor.

Bağlantı isteği herhangi bir IDS/IPS veya firewall engeline takılmıyor ve C&C sunucusuyla 80 portundan bağlantı kuruyor. Eğer takılsaydı ICMP mesajı olarak host unreachable dönecekti ve tekrar CNAME'de belirttiğim adres için tekrar bir DNS sorgusu gönderip gelen IP listesinden bağlanmayı deneyecekti.



TCP bağlantısı kurulur kurulmaz HTTP üzerinden birşeyler çekmeye çalışarak ilk iletişimini yapmış.

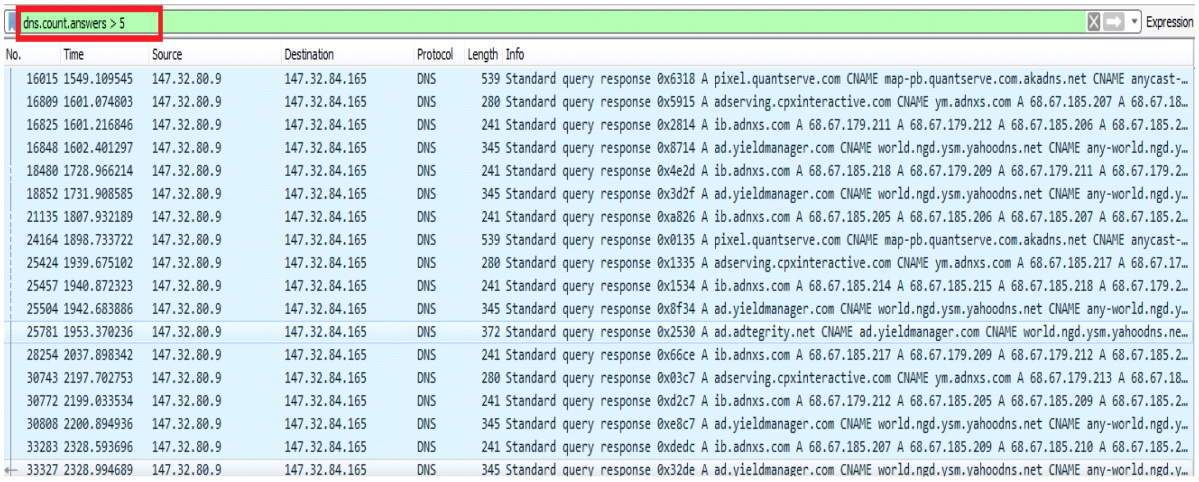
```
GET /service/check2?appid=%7B430FD4D0-B729-4F61-AA34-91526481799D
%7D&appversion=1.3.21.65&applang=&machine=0&version=1.3.21.65&osversion=5.1&servicepack=Service%20Pack%202 HTTP/1.1
User-Agent: Google Update/1.3.21.65;winhttp
X-Last-HR: 0x0
X-Last-HTTP-Status-Code: 0
X-Retry-Count: 0
Host: cr-tools.clients.google.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

HTTP/1.1 204 No Content
Date: Wed, 10 Aug 2011 09:04:27 GMT
Server: GSE
```

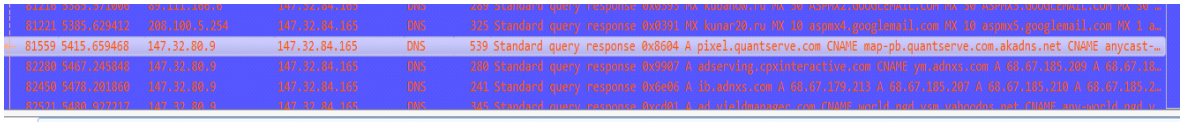
Detaylı olarak incelediğimde, iletişim kurduğu makinanın, uygulamanın versiyon, servis bilgilerini görebiliyorum.

Normal şartlarda sorgudan geri dönen RRs kaydı maksimum 4-5'tir. Bu sayıdan daha fazlası ile karşılaşılırsa tehlikeli bir durum olarak algılanır.

Bende bunun için dns.count.answers > 5 parametresi ile Wiresharkta bu filtreyi uyguladım ve muhtemel tehlikeli cevapları listeledim.



Buna ek olarak çok sayıda tehlikeli olarak nitelendirilen cevapla karşılatığımız için, botnet muhtemelen tek bir komuta kontrol sunucusuna sahip değil, birden fazla sunucuyla bağlantısı var.



Authority RRs: 11

Additional RRs: 3

▷ Queries

◢ Answers

- ▷ pixel.quantserve.com: type CNAME, class IN, cname map-pb.quantserve.com.akadns.net
- ▷ map-pb.quantserve.com.akadns.net: type CNAME, class IN, cname anycast-europe.quantserve.com.akadns.net
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.37
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.43
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.60
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.64
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.15
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.23
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.27
- ▷ anycast-europe.quantserve.com.akadns.net: type A, class IN, addr 95.172.94.28

◢ Authoritative nameservers