

CTU-Malware-Capture-Botnet-43 Pcap Analizi

Pcap dosyasında kayıt altına alınan paketlerin birçoğu 147.32.84.165 IP adresine aitti. Buradan enfekte olmuş bot makinanın bu ipye sahip olduğunu düşünüyorum.

	protocol	packets	bytes	bytes/pkt
0]	total	176064 (100.00%)	33444431 (100.00%)	189.96
1]	ip	175609 (99.74%)	33417131 (99.92%)	190.29
2]	tcp	173112 (98.32%)	33047772 (98.81%)	190.90
3]	ftp	118 (0.07%)	7906 (0.02%)	67.00
3]	ssh	2 (0.00%)	122 (0.00%)	61.00
3]	smtp	16374 (9.30%)	1015188 (3.04%)	62.00
3]	http(s)	23696 (13.46%)	11954989 (35.75%)	504.52
3]	http(c)	48754 (27.69%)	5895234 (17.63%)	120.92
3]	kerb5	56 (0.03%)	59488 (0.18%)	1062.29
3]	netb-se	354 (0.20%)	50178 (0.15%)	141.75
3]	bgp	6607 (3.75%)	441444 (1.32%)	66.81
3]	https	12735 (7.23%)	3927530 (11.74%)	308.40
3]	ms-ds	80 (0.05%)	18603 (0.06%)	232.54
3]	socks	77 (0.04%)	9985 (0.03%)	129.68
3]	kasaa	19 (0.01%)	1168 (0.00%)	61.47
3]	mssql-s	38 (0.02%)	4407 (0.01%)	115.97
3]	scribe	17 (0.01%)	1225 (0.00%)	72.06
3]	squid	90 (0.05%)	5580 (0.02%)	62.00
3]	ms-gc	14 (0.01%)	1041 (0.00%)	74.36
3]	ms-gcs	12 (0.01%)	744 (0.00%)	62.00
3]	mysql	14 (0.01%)	1037 (0.00%)	74.07
3]	irc6667	2354 (1.34%)	168245 (0.50%)	71.47
3]	other	61701 (35.04%)	9483658 (28.36%)	153.70
2]	udp	2379 (1.35%)	359839 (1.08%)	151.26
3]	dns	1594 (0.91%)	286906 (0.86%)	179.99
3]	netb-ns	198 (0.11%)	18827 (0.06%)	95.09
3]	netb-se	106 (0.06%)	24409 (0.07%)	230.27
3]	other	481 (0.27%)	29697 (0.09%)	61.74
2]	icmp	118 (0.07%)	9520 (0.03%)	80.68

tcpdstat ile incelediğim pcap dosyasında paket sayılarını baktığımda saldırının TCP kullanılarak gerçekleştirilmiş ve hedef portu ise HTTP olarak söyleyebiliriz.

http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
624	195.161941	147.32.84.165	137.254.16.78	HTTP	397	GET /jvafx-cache.jnlp HTTP/1.1
652	222.449022	147.32.84.165	94.63.149.152	HTTP	144	GET /rus.php HTTP/1.0
679	231.670214	147.32.84.165	94.63.149.152	HTTP	143	GET /gc.exe HTTP/1.0
805	236.765833	147.32.84.165	60.190.223.75	HTTP	155	GET /p/out/kp.exe HTTP/1.0
818	237.478556	147.32.84.165	94.63.150.52	HTTP	220	GET /orltke/ermgbv.php?adv=adv555&id=1145500768&c=143168975 HTTP/1.1
821	237.483408	147.32.84.165	94.63.150.52	HTTP	220	GET /orltke/caksm1.php?adv=adv555&id=1145500768&c=143168975 HTTP/1.1

GET isteklerini incelediğimde ilk olarak iki adresten exe dosyaları isteniyor. Şüphelendiğim bu exe dosyalarını URL olarak virustotal.com'da tarattığımda zararlı yazılım olarak imzalandığını gördüm.



5 engines detected this URL

URL http://ii.ebatmoyhuy.com/gc.exe
Host ii.ebatmoyhuy.com
Last analysis 2018-08-19 10:27:43 UTC

5 / 67

Detection

Details

Community

Avira

Malware

BitDefender

Malware

Forcepoint ThreatSeeker

Malicious

Kaspersky

Malware

Amaç;

saldırıyı başlatacak bir yazılım olabilir veya ilk kurulan zararlı yazılım packet işlemine sokularak gizlenmiştir, infected makineye kurulum sırasında belirttiğim sitelerden çekilmiş olabilir.

Bu pcap dosyasında servis dışı bırakma saldırısını analiz etmek için tcp.flags.syn == 1 and tcp.flags.ack == 0 filtresini kullandım ve toplam paketlerin %30 kadarını 147.32.84.165 makinası oluşturuyordu. Bot makina 80 portunu hedef alıyordu.

tcp.flags.syn == 1 and tcp.flags.ack == 0						
No.	Time	Source	Destination	Protocol	Length	Info
4548	353.729418	147.32.84.165	67.19.72.206	TCP	62	1519 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4549	353.732617	147.32.84.165	193.23.181.44	TCP	62	1520 → 179 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4550	353.735816	147.32.84.165	174.37.196.55	TCP	62	1521 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4552	353.739026	147.32.84.165	193.23.181.44	TCP	62	1522 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4554	353.742188	147.32.84.165	174.37.196.55	TCP	62	1523 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4556	353.745388	147.32.84.165	174.37.196.55	TCP	62	1524 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4557	353.748605	147.32.84.165	174.37.196.55	TCP	62	1525 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4584	353.864589	147.32.84.165	174.128.246.102	TCP	62	1526 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4585	353.867788	147.32.84.165	193.23.181.44	TCP	62	1527 → 179 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4586	353.870988	147.32.84.165	174.37.196.55	TCP	62	1528 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4588	353.874220	147.32.84.165	67.19.72.206	TCP	62	1529 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4589	353.877415	147.32.84.165	67.19.72.206	TCP	62	1530 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4590	353.880588	147.32.84.165	72.20.15.61	TCP	62	1531 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4591	353.883787	147.32.84.165	174.128.246.102	TCP	62	1532 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4592	353.886990	147.32.84.165	174.128.246.102	TCP	62	1533 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4593	353.890189	147.32.84.165	174.128.246.102	TCP	62	1534 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4594	353.893420	147.32.84.165	72.20.15.61	TCP	62	1535 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4596	353.896625	147.32.84.165	174.128.246.102	TCP	62	1536 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

Packets: 176064 • Displayed: 54255 (30.8%)

Bir diğer saldırı tipi olan ACK Flood' incelemek için kullandığım filtre tcp.flags.ack==1 and ip.src==147.32.84.165

Gelen sonucta paketlerin %30' luk bir kısmını ACK paketleri oluşturuyordu fakat bunun bir servis dışı bırakma saldırısı olduğundan emin olmak için paketler arasındaki süreye bakmam gerekiyordu.

tcp.flags.ack==1 and ip.src==147.32.84.165						
No.	Time	Source	Destination	Protocol	Length	Info
4501	353.587389	147.32.84.165	193.23.181.44	BGP	270	
4502	353.600988	147.32.84.165	193.23.181.44	TCP	60	1413 → 179 [FIN, ACK] Seq=217 Ack=1 Win=64240 Len=0
4503	353.604212	147.32.84.165	193.23.181.44	TCP	60	1414 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4504	353.607405	147.32.84.165	193.23.181.44	HTTP	204	GET / HTTP/1.0
4505	353.617809	147.32.84.165	193.23.181.44	TCP	60	1414 → 80 [FIN, ACK] Seq=151 Ack=1 Win=64240 Len=0
4506	353.621008	147.32.84.165	193.23.181.44	TCP	60	1415 → 179 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4507	353.624189	147.32.84.165	193.23.181.44	BGP	194	
4508	353.634189	147.32.84.165	193.23.181.44	TCP	60	1415 → 179 [FIN, ACK] Seq=141 Ack=1 Win=64240 Len=0
4509	353.637404	147.32.84.165	193.23.181.44	TCP	60	1418 → 179 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4510	353.640589	147.32.84.165	193.23.181.44	BGP	194	
4512	353.650607	147.32.84.165	193.23.181.44	TCP	60	1418 → 179 [FIN, ACK] Seq=141 Ack=1 Win=64240 Len=0
4514	353.653808	147.32.84.165	193.23.181.44	TCP	60	1420 → 179 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4515	353.657004	147.32.84.165	193.23.181.44	BGP	208	
4517	353.667409	147.32.84.165	193.23.181.44	TCP	60	1420 → 179 [FIN, ACK] Seq=155 Ack=1 Win=64240 Len=0
4518	353.670640	147.32.84.165	193.23.181.44	TCP	60	1419 → 179 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Görüldüğü üzere paketler arasındaki süreye bakılarak bir ACK Flood saldırısı yapıldığını söyleyebiliriz.

HTTP GET Flood saldırısı için yaptığım filtrelemede bir sonuç çıkmadı, birde POST için dedim. Enfekte makinadan 184.82.147.251 ip adresine JSON formatında POST isteği atılıyor. Dikkatimi çeken bu durum hakkında kaynak cihazın Cisco olduğunu görüyorum ve bunun bot makinadan C&C sunucusuna gönderilebileceğini düşünüyorum.

ip.src==147.32.84.165 and http.request.method==POST						
No.	Time	Source	Destination	Protocol	Length	Info
1735...	11843.306384	147.32.84.165	184.82.148.43	Destination address 745	POST	/getjson HTTP/1.1 (application/x-www-form-urlencoded)
1738...	11871.403825	147.32.84.165	184.82.148.43	HTTP	745	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1740...	11892.349012	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
1740...	11895.893250	147.32.84.165	184.82.148.43	HTTP	741	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1743...	11928.194888	147.32.84.165	184.82.148.43	HTTP	741	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1745...	11949.380024	147.32.84.165	184.82.148.43	HTTP	741	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1745...	11956.474887	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
1747...	11970.459820	147.32.84.165	184.82.148.43	HTTP	745	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1748...	11981.116022	147.32.84.165	184.82.148.43	HTTP	741	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1750...	12012.600305	147.32.84.165	184.82.155.107	HTTP	743	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1751...	12020.192872	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
1751...	12021.229796	147.32.84.165	184.82.147.251	HTTP	736	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1752...	12033.872109	147.32.84.165	184.82.147.251	HTTP	748	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1754...	12055.444412	147.32.84.165	184.82.147.251	HTTP	748	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1756...	12076.609493	147.32.84.165	184.82.147.251	HTTP	752	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
1757...	12084.004836	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
1758...	12094.403414	147.32.84.165	184.82.147.251	HTTP	752	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)

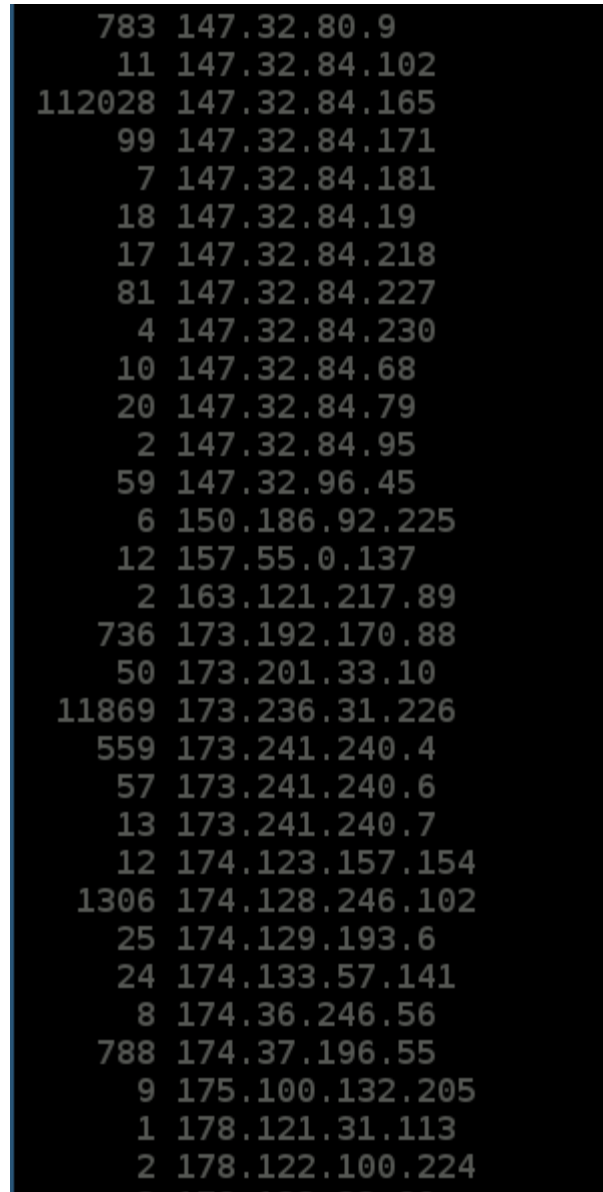
Bu tahminden sonra tekrar POST paketlerini incelediğimde isteklerin tek bir IP adresine değil 2-3 farklı IP adresine de defalarca atıldığını farkettim. Buradan da birden fazla C&C sunucusu olabileceği tahminini yaptım.

http.request.method==POST						
No.	Time	Source	Destination	Protocol	Length	Info
5936	361.669506	147.32.84.165	184.82.155.107	HTTP	739	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
6693	369.901113	147.32.84.165	184.82.155.107	HTTP	743	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
7840	378.126233	147.32.84.165	184.82.155.107	HTTP	739	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
8679	388.768237	147.32.84.165	184.82.148.43	HTTP	709	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
8722	389.558547	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
9583	397.019205	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
10660	405.237569	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
11025	413.453276	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
12393	421.681523	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
13089	429.915224	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
13800	438.139112	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
14850	446.433887	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
15286	449.672507	147.32.84.165	31.192.109.161	HTTP	298	POST /fakedream/index.php HTTP/1.0 (application/x-www-form-urlencoded)
15331	454.683546	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
16852	463.100299	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
17547	471.312859	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
18127	479.806397	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)
19283	488.030867	147.32.84.165	184.82.148.43	HTTP	737	POST /getjson HTTP/1.1 (application/x-www-form-urlencoded)

Pcap dosyasını NetworkMiner ile incelediğimde Images sekmesindeki resimlerden HTTP portuna yapılan istekler neticesinde reklam amaçlı, pop-up tarzı görüntüler çıkarttığını düşündüm.

Yapılan servis dışı bırakma saldırılarında IP spoofing yapılıp yapılmadığını görmek için IP adreslerinin gönderdiği ve aldığı paketlerin sayısını görmek için tcpdump kullanıyorum.

```
tcpdump -n -r ~/Downloads/botnet-capture-20110811-neris.pcap | awk -F" " '{print $3}' | cut -f1,2,3,4 -d"." | sort -n | uniq -c
```



```
783 147.32.80.9
11 147.32.84.102
112028 147.32.84.165
99 147.32.84.171
7 147.32.84.181
18 147.32.84.19
17 147.32.84.218
81 147.32.84.227
4 147.32.84.230
10 147.32.84.68
20 147.32.84.79
2 147.32.84.95
59 147.32.96.45
6 150.186.92.225
12 157.55.0.137
2 163.121.217.89
736 173.192.170.88
50 173.201.33.10
11869 173.236.31.226
559 173.241.240.4
57 173.241.240.6
13 173.241.240.7
12 174.123.157.154
1306 174.128.246.102
25 174.129.193.6
24 174.133.57.141
8 174.36.246.56
788 174.37.196.55
9 175.100.132.205
1 178.121.31.113
2 178.122.100.224
```

Yukarıdaki ekran görüntüsü çıktının küçük bir parçası ve çıkan sonucun geneli aşağı yukarı bu sonuca benzer. Yani IP adreslerinden birden fazla paket gönderilip alınmış.

Bir diğer değişle IP spoofing yapılsaydı bir IP adresi için 1 paket gibi bir durum olabilir. Buradaki sonuca

göre saldırıda IP spoofing yapılmadığı kanaatindeyim.