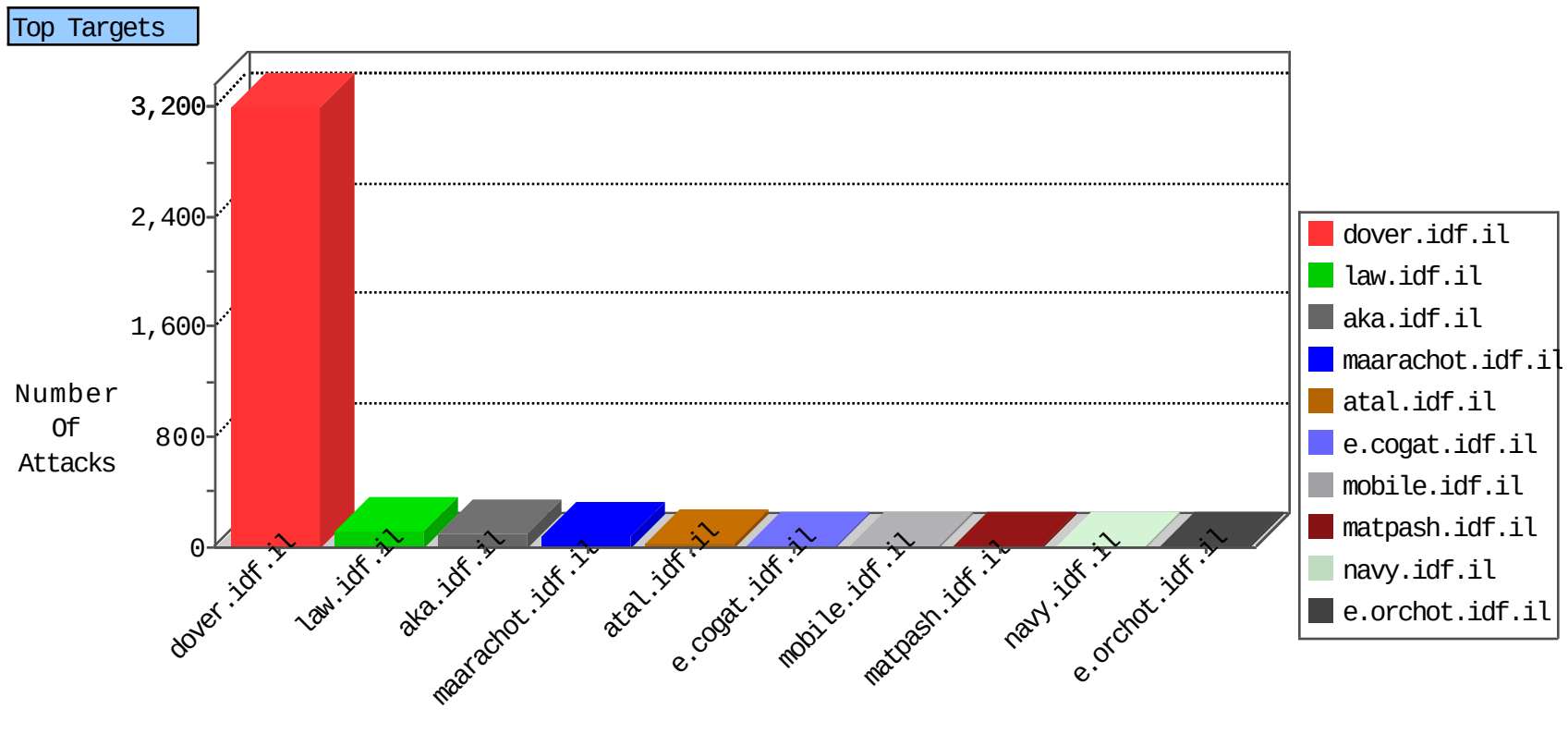
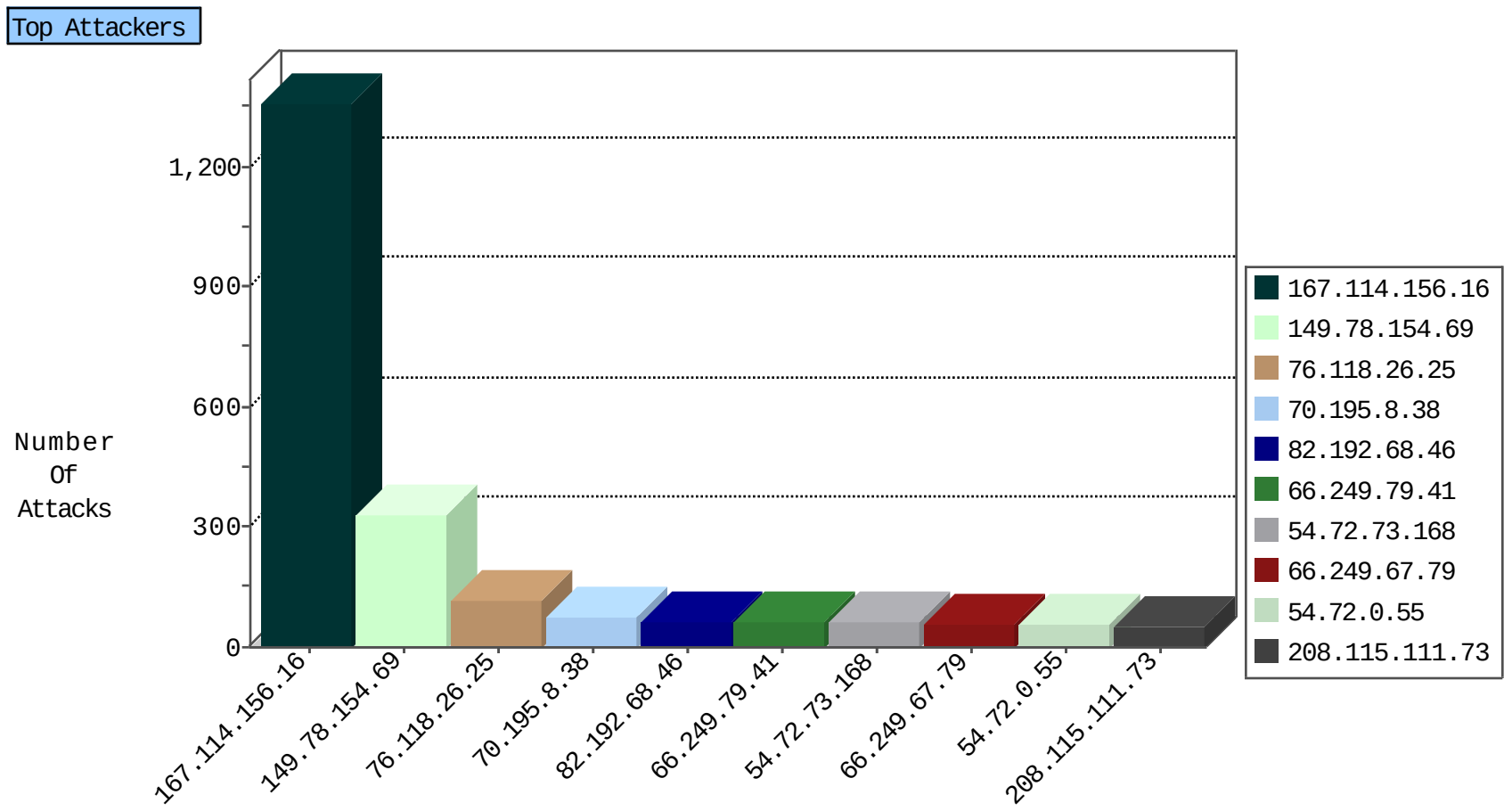
11-05-2015-02:04:09 to 11-05-2015-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-05-2015-02:04:09 to 11-05-2015-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	74644
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	23091
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14984
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9400
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7202
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6039
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4771
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3797
73.136.136.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3191
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3185
131.253.25.190	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2601
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2449
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2004
76.118.26.25	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1701
66.249.83.155	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1631
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1518
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1132
104.10.180.151	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1083
66.249.79.80	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	732
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	388
66.249.79.236	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	361
220.181.108.180	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	268
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	165
62.210.148.246	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	29
46.19.85.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
66.249.83.161	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.54.175.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
54.244.22.103	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4
176.13.23.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.186.90	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
207.46.13.74	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.75.74.41	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.88.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
181.72.226.211	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.244.22.103	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
81.7.15.115	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.88.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
157.55.12.78	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.83.158	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-05-2015-02:04:09 to 11-05-2015-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-05-2015-02:04:09 to 11-05-2015-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-05-2015-02:04:09 to 11-05-2015-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	330
76.118.26.25	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	101
70.195.8.38	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	77
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
209.251.131.167	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
66.249.83.161	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
41.34.188.64	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.83.158	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
109.64.106.99	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
70.196.137.241	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.83.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.249.88.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.65.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	14
176.12.141.131	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
23.240.16.229	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.88.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
154.121.5.247	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
109.186.142.9	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
207.46.13.177	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
31.154.92.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
85.250.118.17	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
64.46.23.242	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
46.19.86.131	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
109.64.101.48	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.93.196	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
131.253.25.250	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.142.137.82	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	6
109.67.136.52	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
213.57.128.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

11-05-2015-02:04:09 to 11-05-2015-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
79.178.30.150	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
79.178.30.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	3
40.77.167.90	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
195.3.144.124	Latvia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/admin.php	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
141.212.122.112	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.112	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
40.77.167.88	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/faq/	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
195.3.144.124	Latvia	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2127-he/cogat.aspx	Block	1
79.241.211.32	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
195.3.144.124	Latvia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.112	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1

11-05-2015-02:04:09 to 11-05-2015-03:04:09