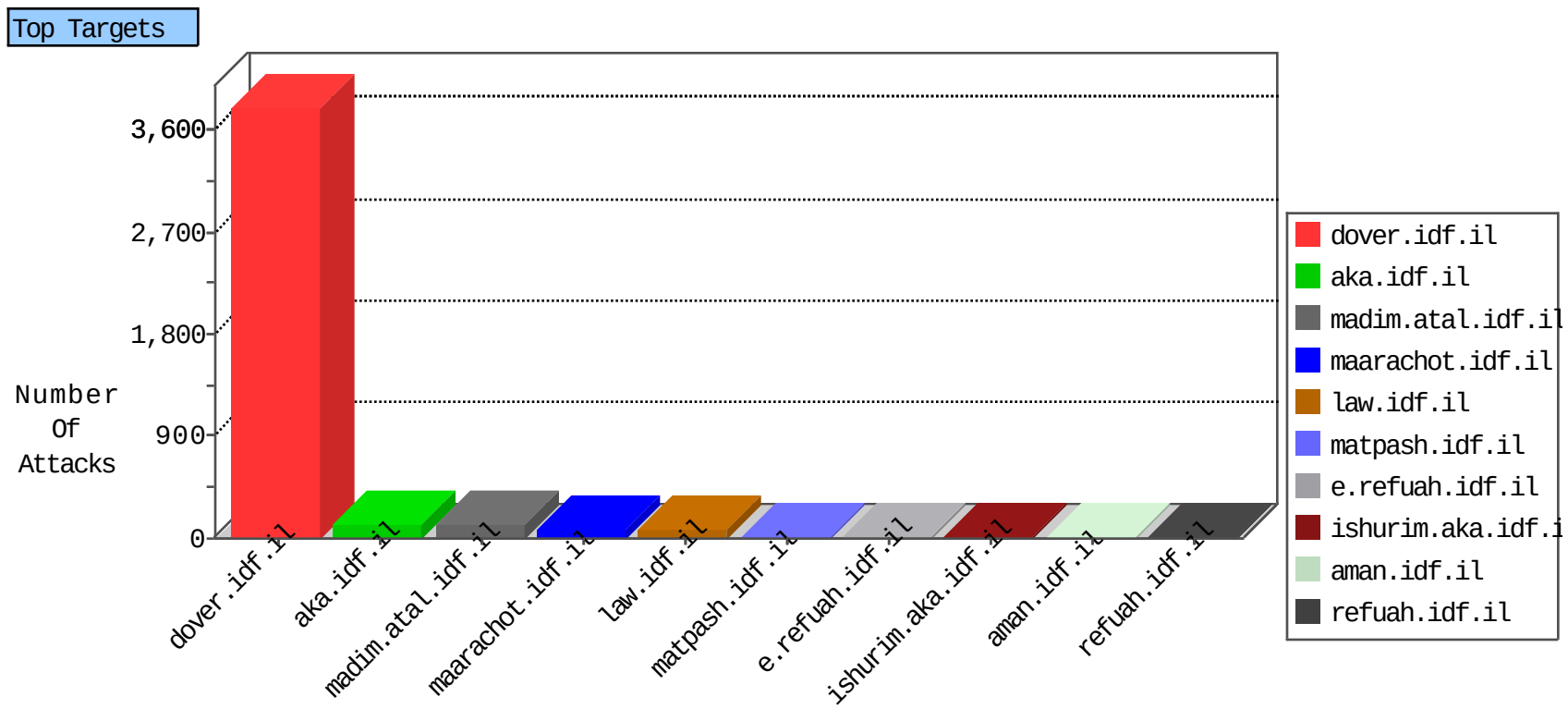
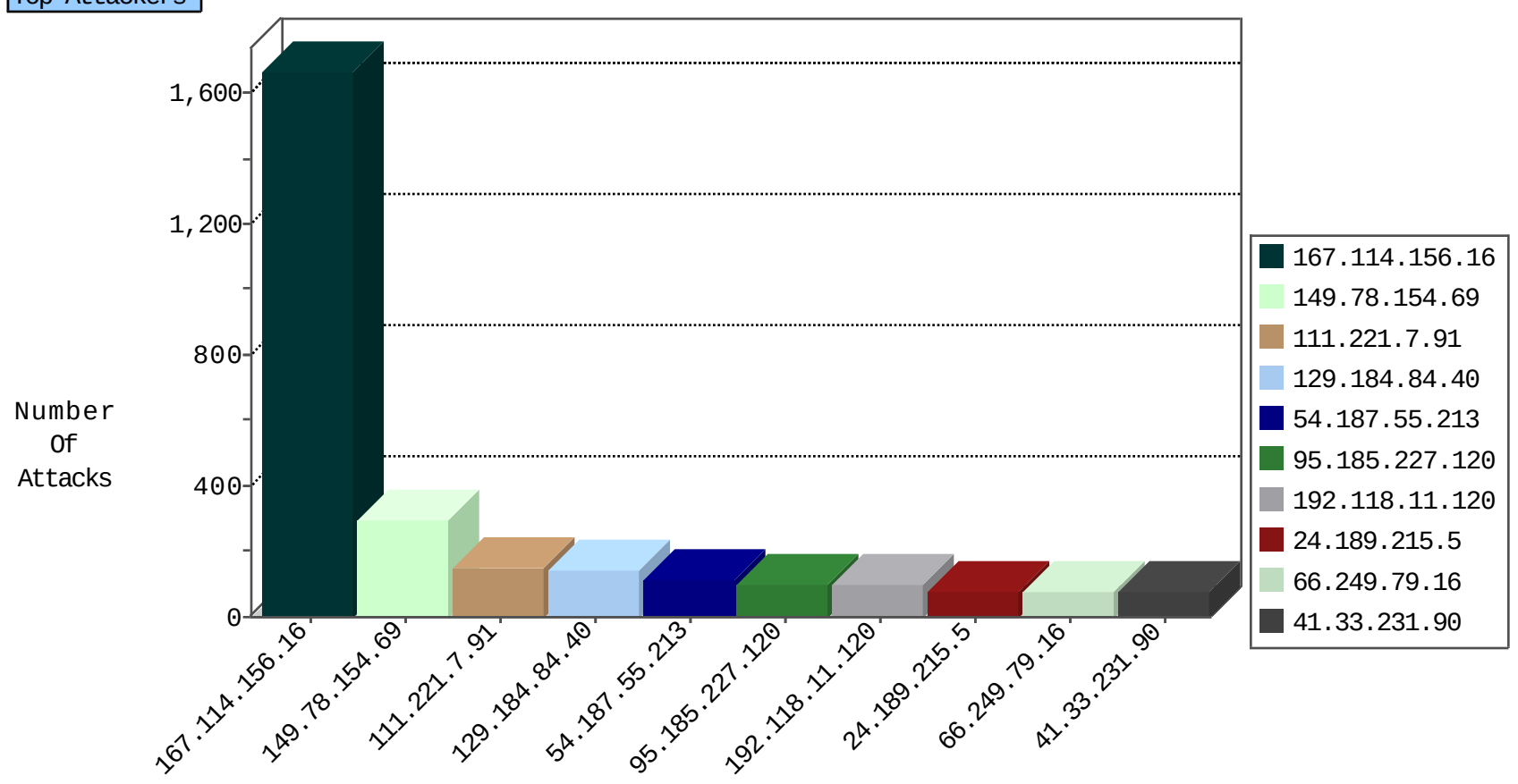
11-05-2015-05:04:02 to 11-05-2015-06:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-05-2015-05:04:02 to 11-05-2015-06:04:02

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	61522
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14460
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12677
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	9508
24.189.215.5	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8081
129.184.84.40	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4177
200.83.42.233	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3177
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3103
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3049
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3009
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2740
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2410
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1399
66.249.88.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1123
66.249.79.232	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	869
207.46.13.180	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	714
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	636
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	593
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	516
95.185.227.120	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
46.19.86.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.54.176.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
66.249.88.101	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
176.12.143.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
222.186.56.42	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
119.130.70.55	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.12.251.37	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
99.238.32.134	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
68.63.30.46	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
222.14.32.127	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
183.160.242.247	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.135.112.218	Germany	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
207.46.13.177	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.179.206.140	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
40.77.167.39	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.186.90	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.10.127.158	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.9.148.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1

11-05-2015-05:04:02 to 11-05-2015-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.138.211	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-05-2015-05:04:02 to 11-05-2015-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.235	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.102.50.56	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.50.56	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

11-05-2015-05:04:02 to 11-05-2015-06:04:02

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.il	drop	First packet isn't SYN	drop	294
111.221.7.91	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	150
129.184.84.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
95.185.227.120	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
24.189.215.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
31.154.94.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
119.130.70.55	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
207.46.13.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
204.12.251.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
99.238.32.134	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.63.30.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
207.46.13.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
200.83.42.233	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
104.179.206.140	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
187.191.7.224	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.88.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.12.143.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.148.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
222.14.32.127	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.88.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
75.20.174.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
157.55.39.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.186.129.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.136.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.106.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

11-05-2015-05:04:02 to 11-05-2015-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.11.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
77.125.108.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
192.118.11.120	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 192.118.11.120	Block	14
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
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
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
188.165.15.235	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	1
87.68.55.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.55.5	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
87.68.55.5	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
141.212.122.112	United States	147.237.72.167	ishurim.aka.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
74.208.105.30	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.67.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/09022011masaiyot.aspx	Block	1
95.79.92.30	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
37.142.226.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.53	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
74.208.105.30	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
107.150.55.52	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.117	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1

11-05-2015-05:04:02 to 11-05-2015-06:04:02