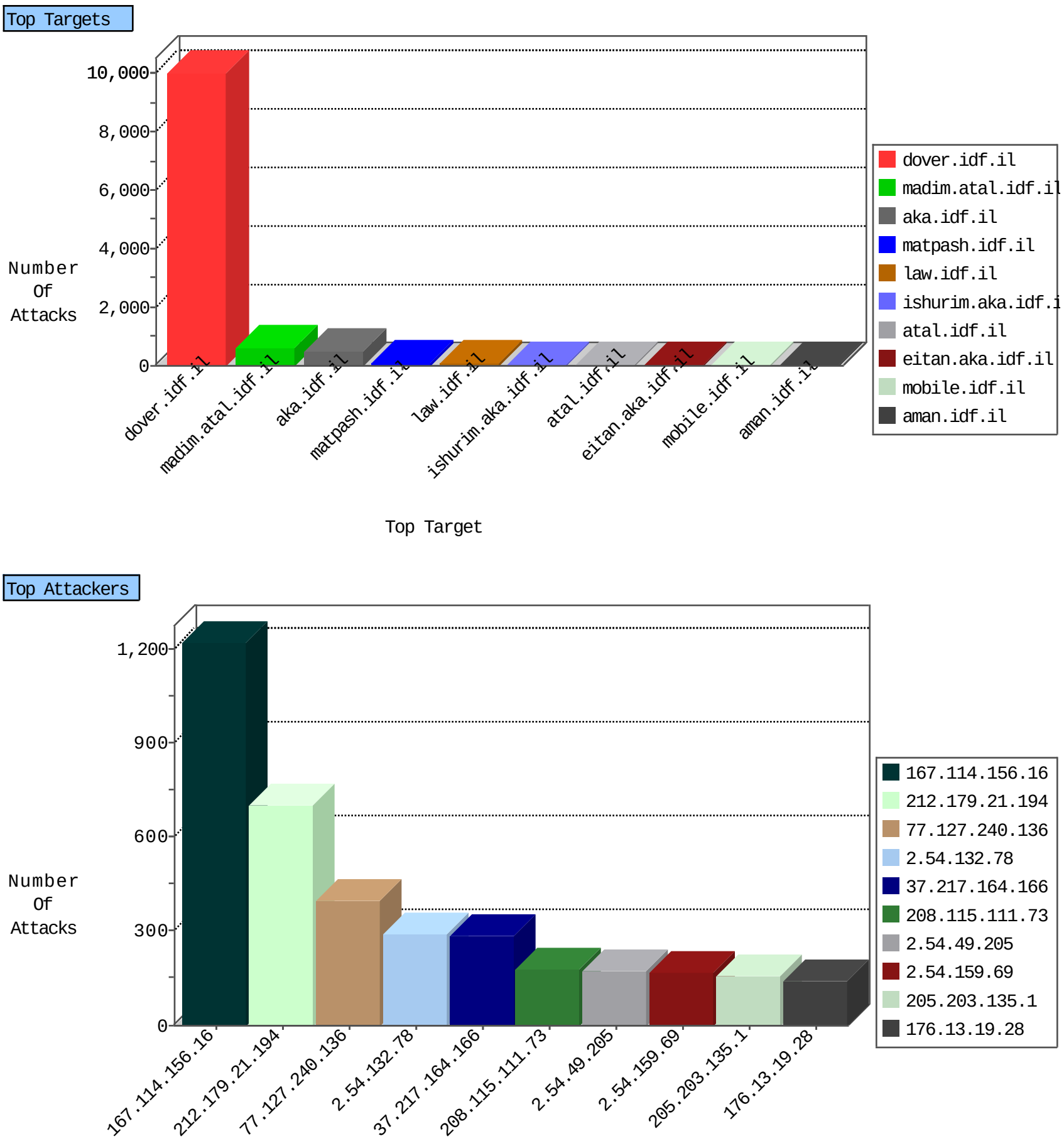
11-05-2015-14:04:09 to 11-05-2015-15:04:09

IDF Under Attack Daily Report



11-05-2015-14:04:09 to 11-05-2015-15:04:09

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	DOS-Tool-SwitchbladG	dest-reset	1853
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	293
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	89
66.249.93.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	69
80.246.136.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	58
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	43
109.160.190.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
149.88.122.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
41.39.21.145	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
132.76.50.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
89.139.29.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
109.66.166.95	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
85.250.203.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
37.26.148.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
87.68.36.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.85.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
82.80.147.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
81.218.198.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
54.198.122.232	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.182.58.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.121.19.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.12.142.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
82.80.21.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
188.247.73.137	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.57.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.66.141.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.183.184.36	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
37.75.210.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.116.145.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
213.149.223.82	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.50.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.121.15.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.170.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.186.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.20.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.76.111.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.116.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
83.149.99.157	Netherlands	147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	5
212.199.121.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.147.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.46.183.247	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.13.195.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.102.197.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
217.66.232.4	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

11-05-2015-14:04:09 to 11-05-2015-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.44.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-05-2015-14:04:09 to 11-05-2015-15:04:09

Top Attackers In IDS

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

11-05-2015-14:04:09 to 11-05-2015-15:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	689
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	397
37.217.164.166	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	283
2.54.49.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	172
2.54.159.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	166
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	164
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	127
85.65.236.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
196.207.233.184	Senegal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
79.183.179.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
5.108.144.164	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
212.179.57.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.45.134.151	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
82.166.87.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
85.250.203.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
212.76.111.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
188.53.152.162	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
5.28.188.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
87.68.147.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
79.183.116.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
2.52.174.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
110.22.140.127	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.0.238.61	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
50.23.99.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.148.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
81.218.198.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
31.154.92.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
80.246.136.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
185.99.32.2		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.62.82		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36

11-05-2015-14:04:09 to 11-05-2015-15:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.132.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.132.78	Block	169
176.13.19.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.54.132.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
176.13.19.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
79.180.52.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.19.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
176.13.19.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.132.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.132.78	Block	16
176.12.138.179	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.175.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	3
85.250.110.226	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
79.182.55.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.110.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
85.250.203.117	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
62.210.88.201	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
85.65.84.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.207.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.120.102	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
216.223.27.24	United States	147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
185.32.179.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
109.66.4.121	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
37.238.120.65	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
5.28.149.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
84.109.90.213	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.45.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
194.114.146.227	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
62.219.99.130	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
31.154.91.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
2.54.179.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.223.27.26	United States	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
185.107.48.3		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/112293.pdf	Block	1
5.28.180.185	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
84.109.90.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
196.207.233.184	Senegal	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.asp	Block	1
37.8.80.173	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
217.31.48.30	Czech Republic	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/rom-0	Block	1
79.182.223.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.184.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
185.120.126.1		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	1
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.102.93	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/509-he/patzar.aspx	Block	1

11-05-2015-14:04:09 to 11-05-2015-15:04:09