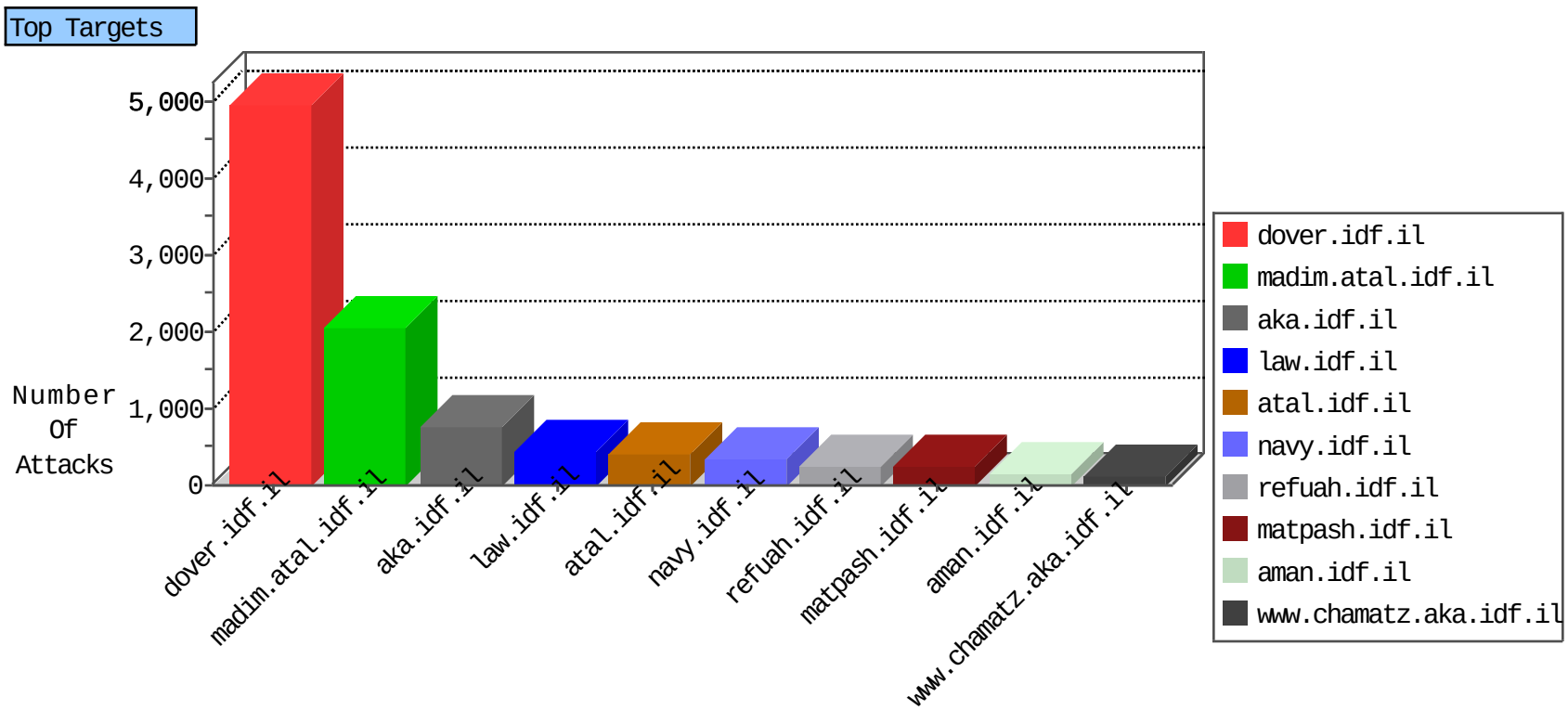
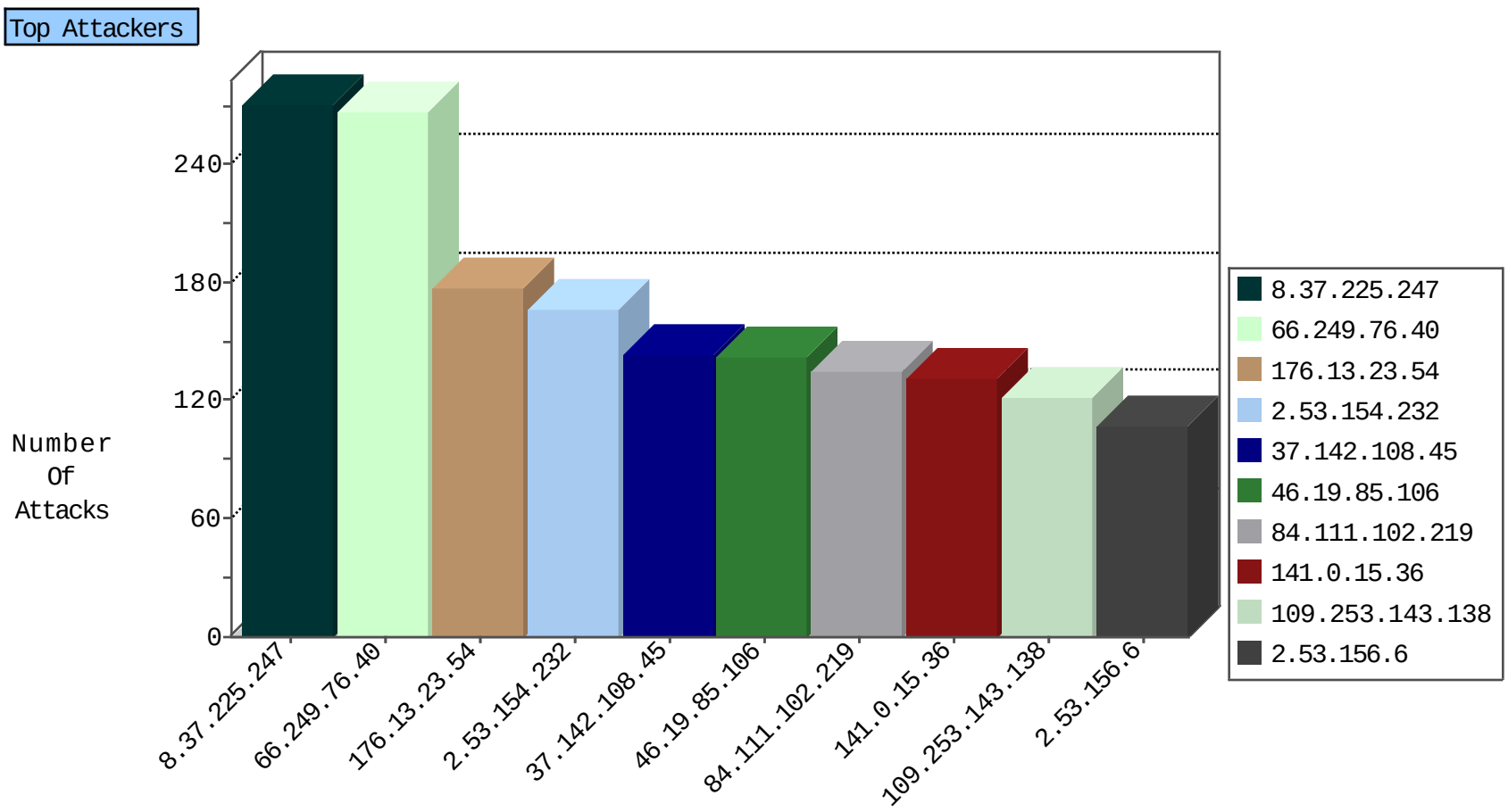
09-03-2016 to 09-04-2016

IDF Under Attack Daily Report





09-03-2016 to 09-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	47
46.19.85.171	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	34
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
85.250.136.18	Israel	147.237.72.166	aka.idf.il	L4 Source or Dest Port Zero	drop	15
77.139.159.97	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
79.176.139.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
149.56.41.137	United States	147.237.77.74	law.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	12
109.253.230.172	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
5.102.104.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9
85.250.136.18	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
84.108.118.243	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.117.245.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
8.37.225.75	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
46.19.86.228	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
105.158.179.65	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
66.240.219.146	United States	147.237.76.30	himush.idf.il	TCP handshake violation, first packet not syn	drop	3
79.180.55.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.247	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Black List	drop	2
122.114.102.90	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
109.236.84.10	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	2
190.13.55.190	Colombia	147.237.77.170	maarachot.idf.il	Invalid L4 Header Length	drop	2
109.253.230.172	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.67.239.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
217.23.9.123	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	2
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	2
8.37.225.247	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
120.132.50.135	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
84.111.119.121	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.42	refuah.idf.il	Black List	drop	2
5.28.158.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.111.119.121	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
117.21.191.2	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
71.6.158.166	United States	147.237.76.86	navy.idf.il	Black List	drop	1
185.25.33.139	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.230.107.174	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1
209.126.103.42	United States	147.237.76.30	himush.idf.il	Black List	drop	1
46.19.85.91	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
5.79.68.131	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
118.193.22.198	Hong Kong	147.237.76.148	gqcenter.aka.idf.i	Black List	drop	1

09-03-2016 to 09-04-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016 to 09-04-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.40	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	267
149.56.41.137	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	76
212.68.146.35	147.237.77.226	Israel	www.chamatz.aka.idf.il	SQL Injection - Select From	54
209.208.126.125	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	54
87.106.184.160	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	53
83.168.250.50	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	48
213.174.55.11	147.237.0.34	Germany	tikshuv.idf.il	SQL Injection - Select From	38
213.60.255.71	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	36
64.87.23.55	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	26
94.73.145.50	147.237.77.176	Turkey	matpash.idf.il	SQL Injection - Select From	26
81.88.48.113	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	22
40.85.96.77	147.237.77.233	Ireland	atal.idf.il	SQL Injection - Select From	20
50.63.197.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
74.208.230.195	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
184.168.46.74	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
83.168.250.50	147.237.76.31	Sweden	nakchal.idf.il	SQL Injection - Select From	20
188.165.250.173	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	20
74.208.192.137	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	20
65.39.128.237	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
195.8.208.118	147.237.76.42	Netherlands	refuah.idf.il	SQL Injection - Select From	20
212.147.60.96	147.237.76.86	Switzerland	navy.idf.il	SQL Injection - Select From	20
216.249.107.200	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
177.185.192.85	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	18
194.88.154.131	147.237.76.42	Poland	refuah.idf.il	SQL Injection - Select From	18
96.251.45.13	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
24.222.4.86	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	18
71.227.10.76	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
96.251.45.13	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
216.119.125.34	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	17
213.203.215.16	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	16
66.249.81.212	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	16
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	16
173.0.129.149	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
187.188.169.247	147.237.77.74	Mexico	law.idf.il	SQL Injection - Select From	14
216.119.125.57	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
85.136.227.77	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	8
184.168.192.31	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
204.93.196.218	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	8
23.91.70.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
195.8.208.130	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	8
71.171.93.66	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	8
79.170.196.68	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
205.144.171.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
38.110.11.92	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
85.94.76.17	147.237.77.74	Croatia	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8

09-03-2016 to 09-04-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
141.0.15.36	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
62.128.48.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
109.253.217.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
141.226.217.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
176.13.236.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
109.253.230.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
79.180.169.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
8.37.225.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
79.177.52.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
37.142.231.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	54
84.108.147.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
79.180.192.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
79.181.234.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
213.57.184.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.117.217.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.65.79.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.66.147.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
5.29.211.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
77.139.74.137	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
87.70.32.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.117.132.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
84.229.22.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
37.142.209.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
46.19.85.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
176.13.229.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
141.0.14.74	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.64.184.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
84.108.188.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.85.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.138.64.130	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.250.80.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
79.178.143.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.146.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.53.54.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
79.179.16.221	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
5.102.104.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
46.33.32.2	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
178.197.239.213	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
217.132.127.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	29
68.197.228.235	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	177
2.53.154.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	166
37.142.108.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	142
84.111.102.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
109.253.143.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
2.53.156.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.53.187.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
109.253.136.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
2.53.152.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
82.80.166.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
109.253.215.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.67.188.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
37.26.146.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
2.53.186.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
2.53.4.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
109.67.192.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.65.66.120	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.65.66.120	Block	37
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
109.66.105.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.53.135.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
121.9.141.166	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.141.166	Block	17
212.40.139.39	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	16
65.55.210.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	16
109.67.199.85	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.199.85	Block	16
175.44.17.151	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 175.44.17.151	Block	15
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	14
37.26.146.169	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	14
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
141.226.240.212	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
199.30.24.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
84.108.27.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.64.176.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
199.30.24.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
117.26.117.51	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
109.65.184.162	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
117.26.117.51	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 117.26.117.51	Block	8
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
185.32.179.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.190.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
175.44.17.151	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	6
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	6
149.56.41.137	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 149.56.41.137	Block	6
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6

09-03-2016 to 09-04-2016