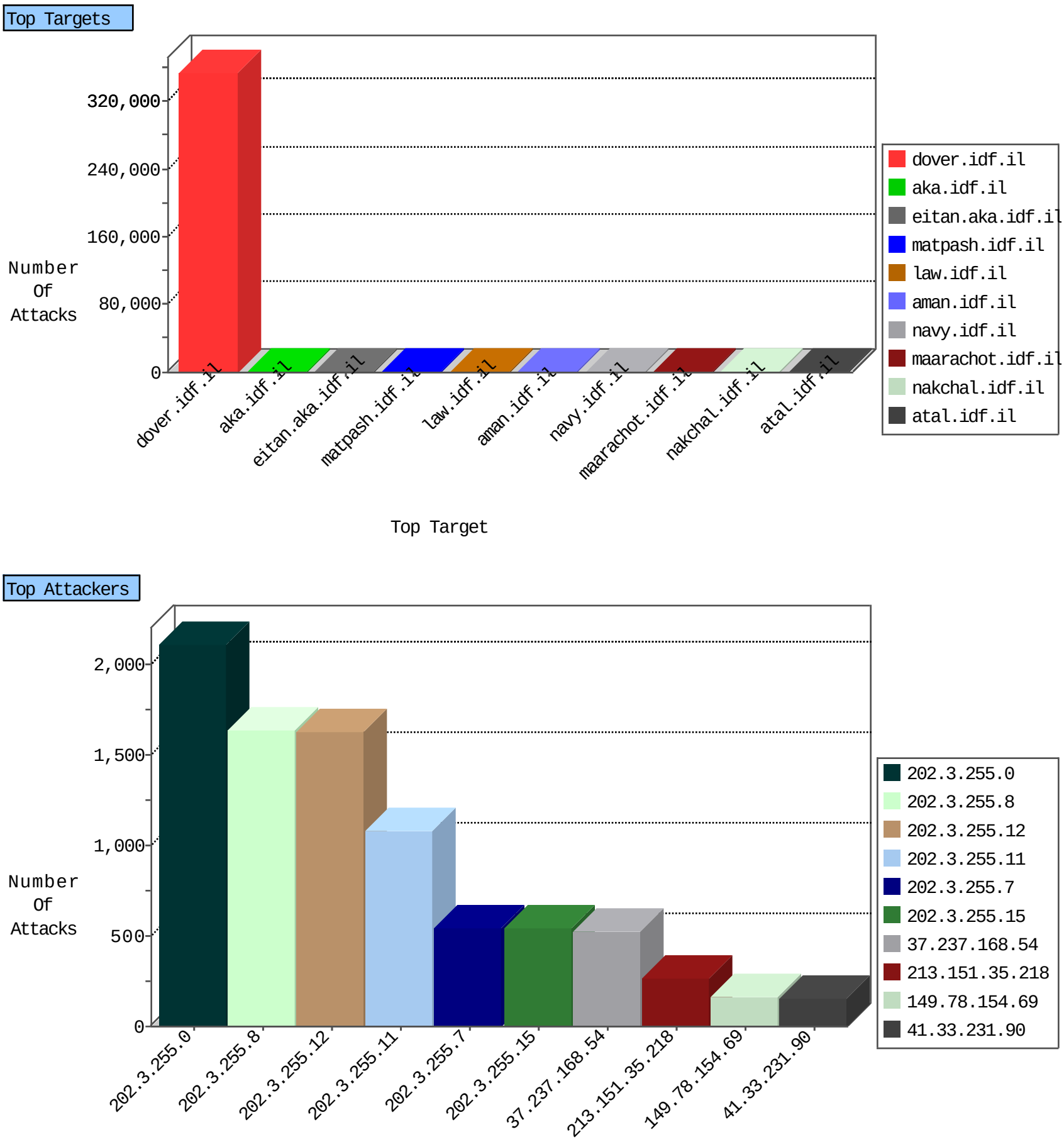
11-10-2015-05:04:08 to 11-10-2015-06:04:08

IDF Under Attack Daily Report



11-10-2015-05:04:08 to 11-10-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.57.135.103	Uruguay	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5779
66.249.64.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3314
192.222.192.79	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2940
60.71.143.69	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2911
71.212.94.123	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2706
104.138.32.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2570
50.91.23.122	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2500
66.249.64.153	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1768
112.21.27.114	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	530
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	355
175.249.218.126	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	350
186.250.47.110	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	219
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	170
175.16.174.27	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	147
187.90.38.91	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	139
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	136
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	133
46.38.235.88	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	130
58.252.11.103	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
183.118.226.65	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	119
182.128.41.14	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	93
117.221.189.31	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	91
117.202.62.45	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	83
114.83.32.71	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	78
37.12.210.88	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	74
113.61.15.43	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
120.187.86.6	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
179.243.248.79	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	72
126.62.243.94	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	72
175.238.3.88	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70
1.230.0.100	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70
120.188.140.21	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68
150.42.202.43	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
115.202.126.62	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
190.22.21.54	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
126.190.80.125	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57
188.128.224.58	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	55
125.85.4.79	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
171.15.61.4	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
61.76.227.23	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	51
175.112.66.100	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	49
144.255.0.89	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
125.24.0.117	Thailand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
58.246.226.53	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
1.231.186.104	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
186.180.126.65	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
126.191.11.27	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
110.244.247.9	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
1.250.72.21	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
110.12.0.66	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36

11-10-2015-05:04:08 to 11-10-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-10-2015-05:04:08 to 11-10-2015-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.0	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1972
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1533
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1521
202.3.255.11	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1011
202.3.255.7	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	508
202.3.255.15	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	504
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
157.231.88.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.76.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.208.125	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.198.185.86	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.29.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.61.92	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.140.57	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.148.77.122	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.183.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.64.48	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.68.70	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.114.126	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.13.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.209.91	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.202.97.22	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.167.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.12.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.131.49	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.102.77	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.158.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.28.68	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.170.115	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.88.37.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.4.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.222.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.40.92	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.95.222.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.95.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.213.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.20.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.192.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.185.44	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.199.146.121	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.130.167.22	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.126.137.69	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
170.106.58.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.248.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.42.7	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.63.245.65	147.237.77.216	Portugal	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.86.24	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-10-2015-05:04:08 to 11-10-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.237.168.54	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	520
213.151.35.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	263
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
99.127.169.246	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
37.217.181.160	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
79.182.211.31	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
172.56.14.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
203.27.38.40	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
207.46.13.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.67.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
94.197.121.26	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
207.46.13.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	26
74.136.65.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.46.13.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.185.4.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
75.181.80.229	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
88.198.25.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
162.243.73.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.231.208.114	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
201.141.103.180	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
209.6.148.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
40.77.167.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.210.107.201	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

11-10-2015-05:04:08 to 11-10-2015-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	8
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.244	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/iturim/asp/searchresults.asp	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
207.46.13.142	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
186.144.97.250	Colombia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19265-he/dover.aspx	Block	1
5.141.213.6	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.166	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.64.204.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
194.144.114.156	Iceland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
46.117.222.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
157.55.39.64	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.79.104	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8865-he/refuah.aspx	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main/	Block	1
157.55.39.146	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
207.46.13.75	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1

11-10-2015-05:04:08 to 11-10-2015-06:04:08