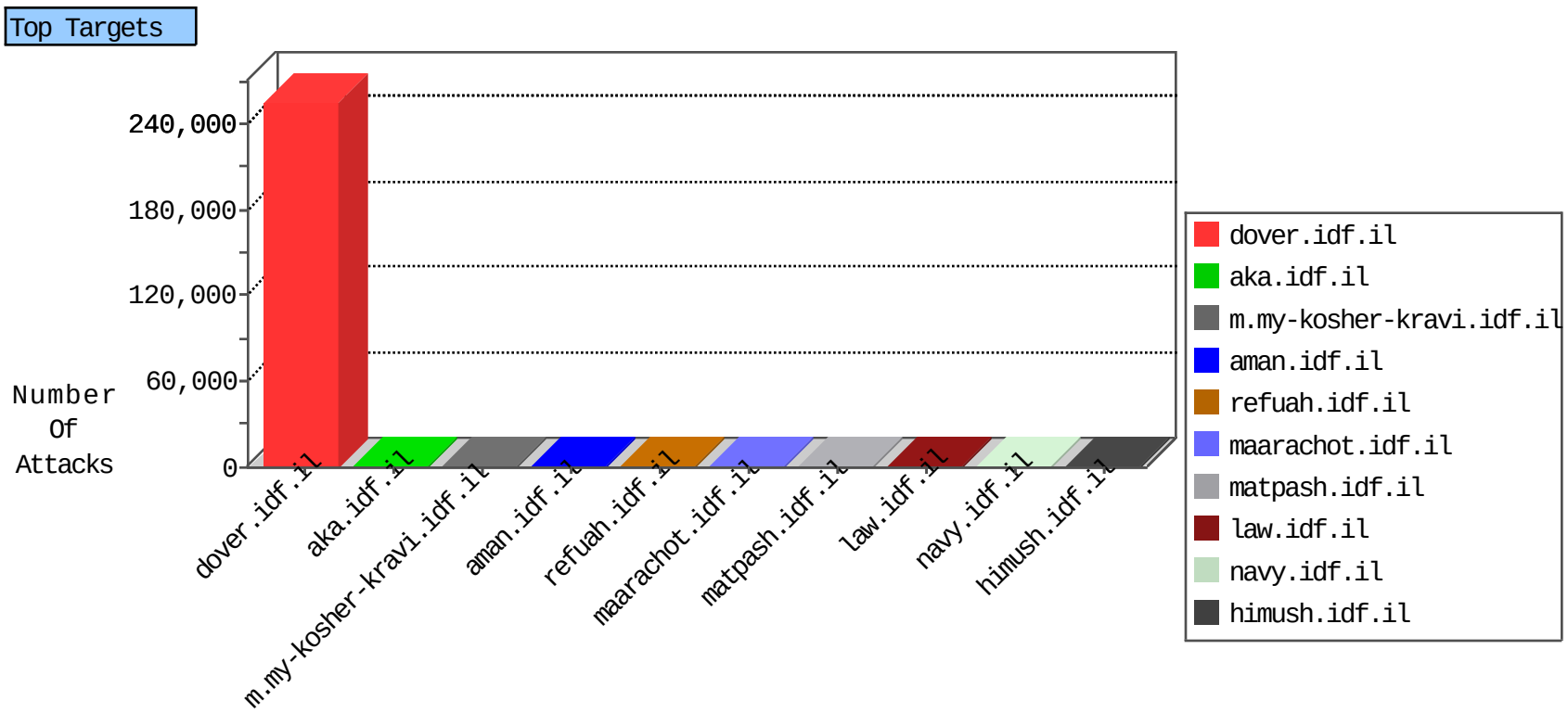
11-18-2015-05:04:08 to 11-18-2015-06:04:08

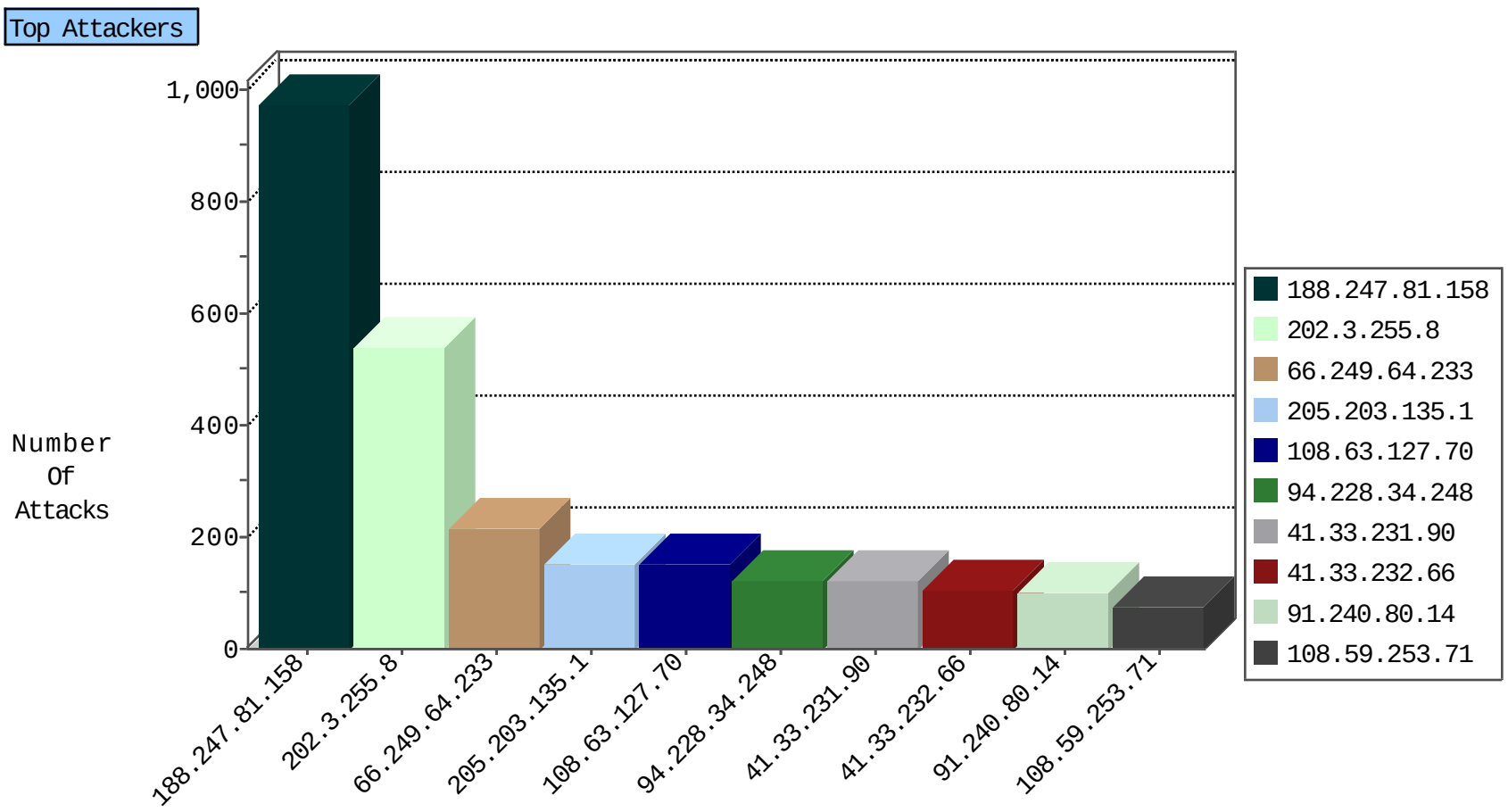
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-18-2015-05:04:08 to 11-18-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.224.133.26	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5864
41.47.62.141	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2903
123.97.143.82	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2864
222.235.7.48	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2827
188.154.129.101	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2669
126.145.55.107	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2598
112.176.249.42	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2558
134.178.186.46	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2521
223.200.124.17	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	454
17.178.58.47	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	266
218.77.100.106	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	251
96.114.240.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	244
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	220
147.248.49.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	218
219.64.76.84	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	216
83.73.198.48	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	189
106.82.82.119	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	169
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	168
177.60.167.111	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	156
120.164.231.42	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	154
191.204.189.26	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	135
59.88.28.101	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	122
133.64.142.23	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
92.112.110.2	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79
178.78.235.6	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	72
67.215.222.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
126.218.151.99	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
133.14.204.19	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	49
1.176.72.19	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
84.209.243.75	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
70.79.16.118	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.186.48.67	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.32.92	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.169.73.35	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.221.222.38	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
24.148.122.68	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.105.26.24	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.80.157.58	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.61.27.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
121.0.27.32	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
63.248.3.114	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
112.255.178.23	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
193.90.109.125	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
23.91.253.8	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.17.89.4	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
161.46.154.98	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
149.88.191.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
216.181.228.10	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-18-2015-05:04:08 to 11-18-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-18-2015-05:04:08 to 11-18-2015-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	502
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
167.97.84.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.205.88.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.178.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.66.90	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.255.125	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.199.132.77	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
216.151.197.118	147.237.77.216	Hong Kong	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.117.126	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.151.78.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.76.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.240.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.20.175.119	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.239.91	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.145.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.226.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.169.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.165.107	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.223.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.182.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.232.168.3	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.227.86.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.251.103	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.171.104	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
192.43.159.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.77.9	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.200.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.58.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.147.93	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.144.2.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.157.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.77.128.236	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.127.29.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.29.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.44.231.50	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.121.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.174.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.22.79	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.243.5	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.81.94	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.77.128.236	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.212.100.6	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.18.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.64.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.170.94	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.0.26	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.77.128.236	147.237.76.31		nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-18-2015-05:04:08 to 11-18-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.247.81.158	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	974
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	170
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
108.63.127.70	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	150
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	120
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
54.159.7.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
91.240.80.14	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
70.215.9.246	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
52.29.51.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
113.197.14.2	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
108.220.246.28	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
41.47.62.141	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
204.13.200.200	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
198.1.101.123	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
158.69.2.151	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
52.33.202.208	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
54.81.101.210	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
178.63.165.187	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	19
76.106.42.50	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
66.249.64.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
40.77.167.84	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
114.108.217.180	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
65.19.138.33	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
24.218.80.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
40.77.167.97	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
69.126.164.199	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
104.131.197.228	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

11-18-2015-05:04:08 to 11-18-2015-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.193	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
176.13.1.0	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.1.0	None	3
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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
79.181.66.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
23.20.238.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.181.66.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/ajax/pages/fan_status.php	Block	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/2690.jpg	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.117.237.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
212.76.110.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	1
62.25.16.234	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/localauth/setaccount.aspx	Block	1
141.212.121.192	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
216.218.206.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
176.13.1.0	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding in4IWIsJ_P	None	1

11-18-2015-05:04:08 to 11-18-2015-06:04:08