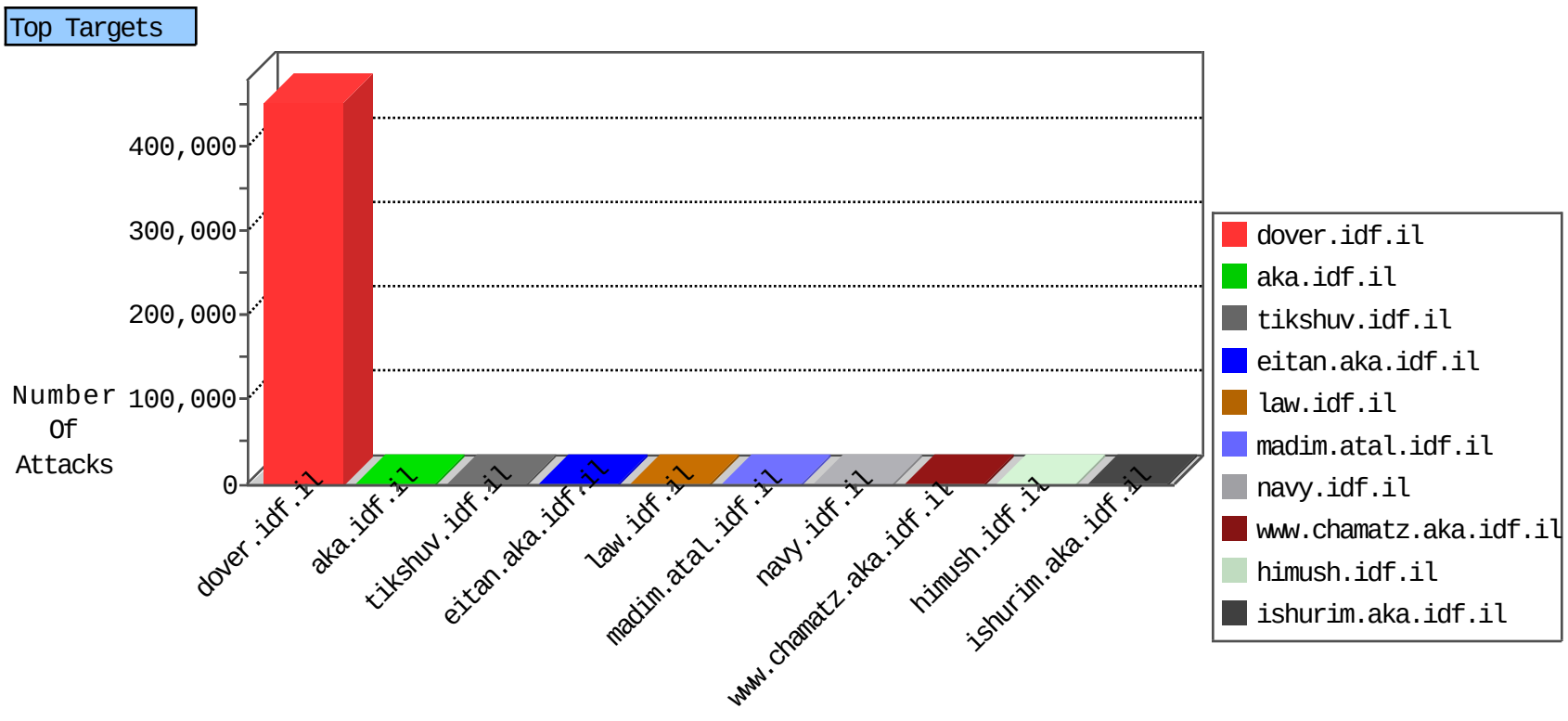
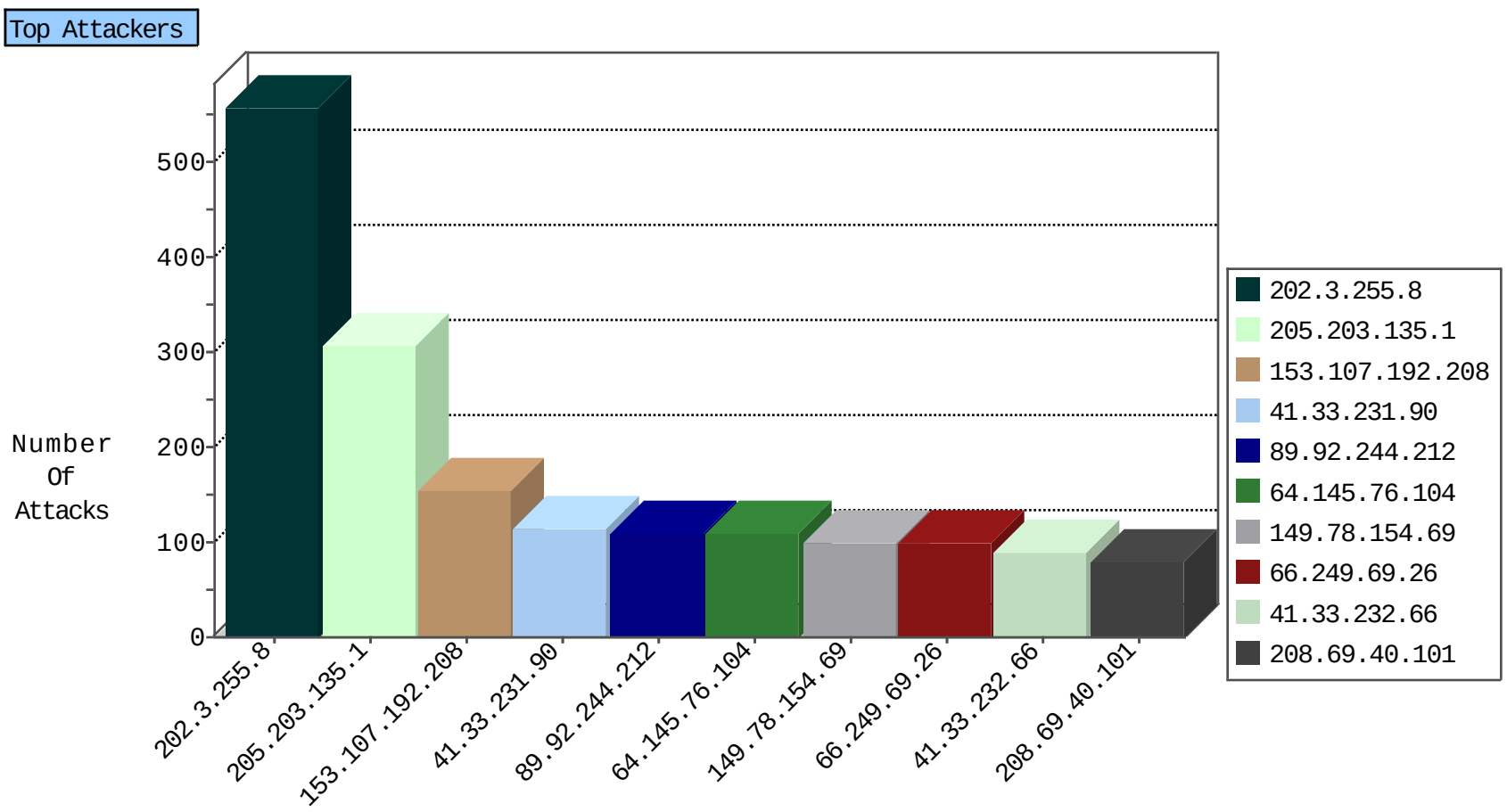
11-17-2015-02:04:09 to 11-17-2015-03:04:09

IDF Under Attack Daily Report





11-17-2015-02:04:09 to 11-17-2015-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3222
178.223.70.28		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3151
66.249.67.237	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	3116
82.52.179.116	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2839
95.102.107.119	Slovakia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2773
150.83.17.123	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2713
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1964
210.69.15.88	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	398
119.234.4.54	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	349
122.116.42.41	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	307
158.245.194.2	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	264
82.25.0.37	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	256
117.221.247.18	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	174
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	170
184.178.220.62	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	146
124.127.206.113	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	107
126.216.196.84	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	102
106.242.248.70	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68
133.64.147.110	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	26
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
192.116.177.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
198.200.85.92	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.255.133.87	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
70.51.36.155	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
78.33.93.124	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.135.157.105	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
24.46.78.76	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
178.20.83.15	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
193.169.44.62	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
83.168.69.111	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
222.186.30.215	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
63.248.210.27	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
24.149.51.112	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.168.72.11	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.211.245.33	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
100.38.147.43	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.110.200.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.234.5	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
17.141.58.70	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
126.178.53.19	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
76.77.224.79	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.58.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
92.254.199.32	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
189.144.218.63	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
50.199.45.120	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.104.158.57	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
70.63.47.80	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
114.36.172.66	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-17-2015-02:04:09 to 11-17-2015-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.130	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	7
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.131	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.108	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-17-2015-02:04:09 to 11-17-2015-03:04:09

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	520
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
157.232.253.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.198.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.218.223.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.100.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.199.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
121.46.117.74	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.224.179.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.126.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.112.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.172.108	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.45.39.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.86.118	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.176.60	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.52.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.231.79.75	147.237.77.216	Colombia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.89.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.95.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.181.3	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.203.15.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.197.32	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.170.35	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.166.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.140.87	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.20.20.27	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.24.27	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.63.16	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.10.74.196	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
209.198.183.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.182.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.250.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.33.92	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.120.123	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.194.191.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.94.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.21.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.169.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.104.15	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.201.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.216.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.10.74.196	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
209.145.16.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.68.83	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.133.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.198.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.87.18	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.147.242.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.28.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-17-2015-02:04:09 to 11-17-2015-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	306
153.107.192.208	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	154
89.92.244.212	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	109
64.145.76.104	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	78
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	71
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
2.136.170.13	Spain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
52.33.66.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
109.67.119.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
209.6.148.106	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
82.165.137.121	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
66.87.103.14	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
62.44.134.88	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
37.26.148.246	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
153.107.97.170	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
207.46.13.64	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
100.38.183.54	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
146.111.147.57	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
66.249.69.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
5.29.122.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
5.29.122.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
52.34.39.186	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
157.55.39.119	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	19
66.249.69.42	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
37.26.147.234	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
179.28.66.132	Uruguay	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	13
108.180.216.191	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
174.67.122.2	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
139.162.216.112	Netherlands	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

11-17-2015-02:04:09 to 11-17-2015-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.71	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.130.71	Block	9
176.12.146.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
176.13.1.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
83.199.126.107	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.151.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
141.212.122.80	United States	147.237.77.234	halag.idf.il	Multiple Malformed URL from 141.212.122.80	Block	1
37.237.192.46	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
167.57.173.23	Uruguay	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
40.77.167.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
54.224.45.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
80.246.130.71	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
128.252.173.121	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.80	United States	147.237.76.30	himush.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8906-he/refuah.aspx	Block	1
5.189.163.161	Germany	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1

11-17-2015-02:04:09 to 11-17-2015-03:04:09