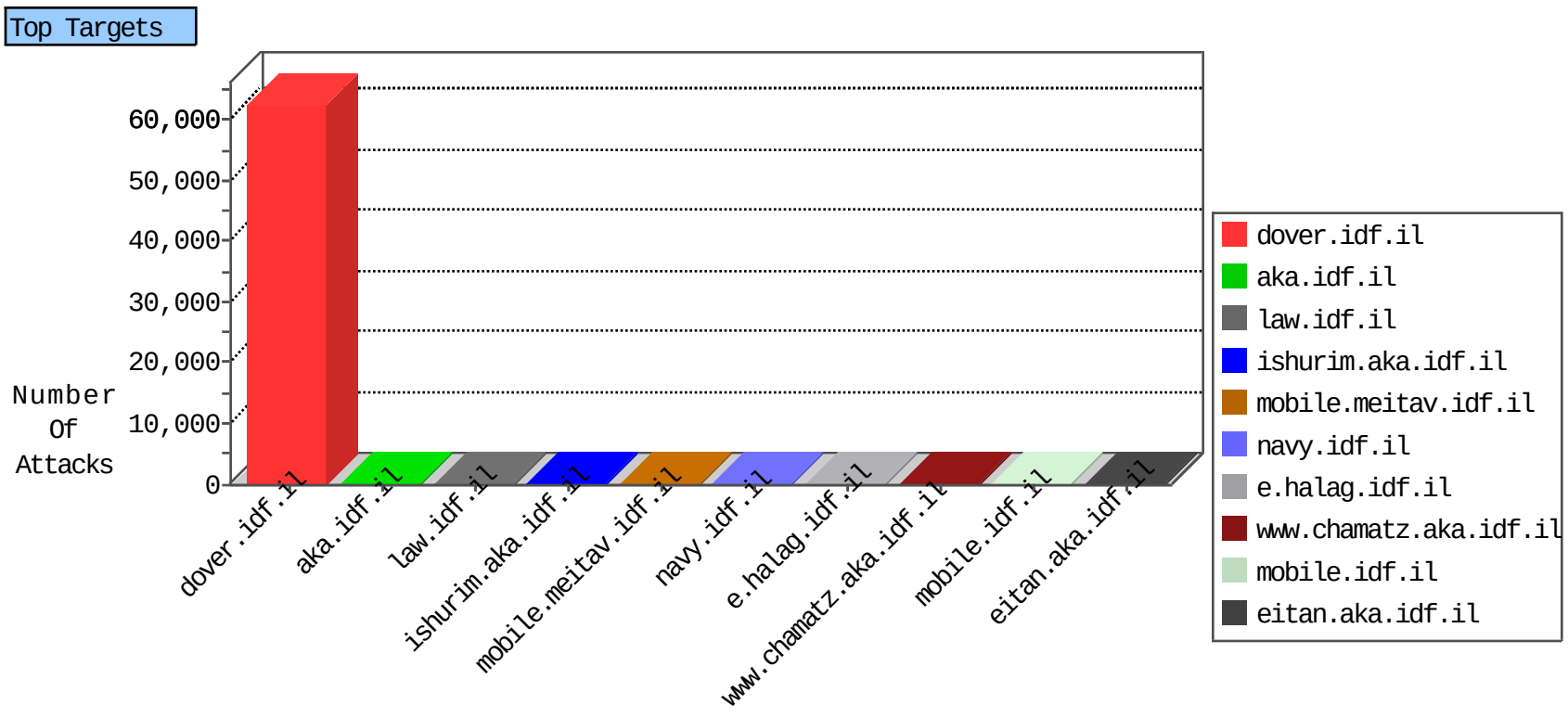
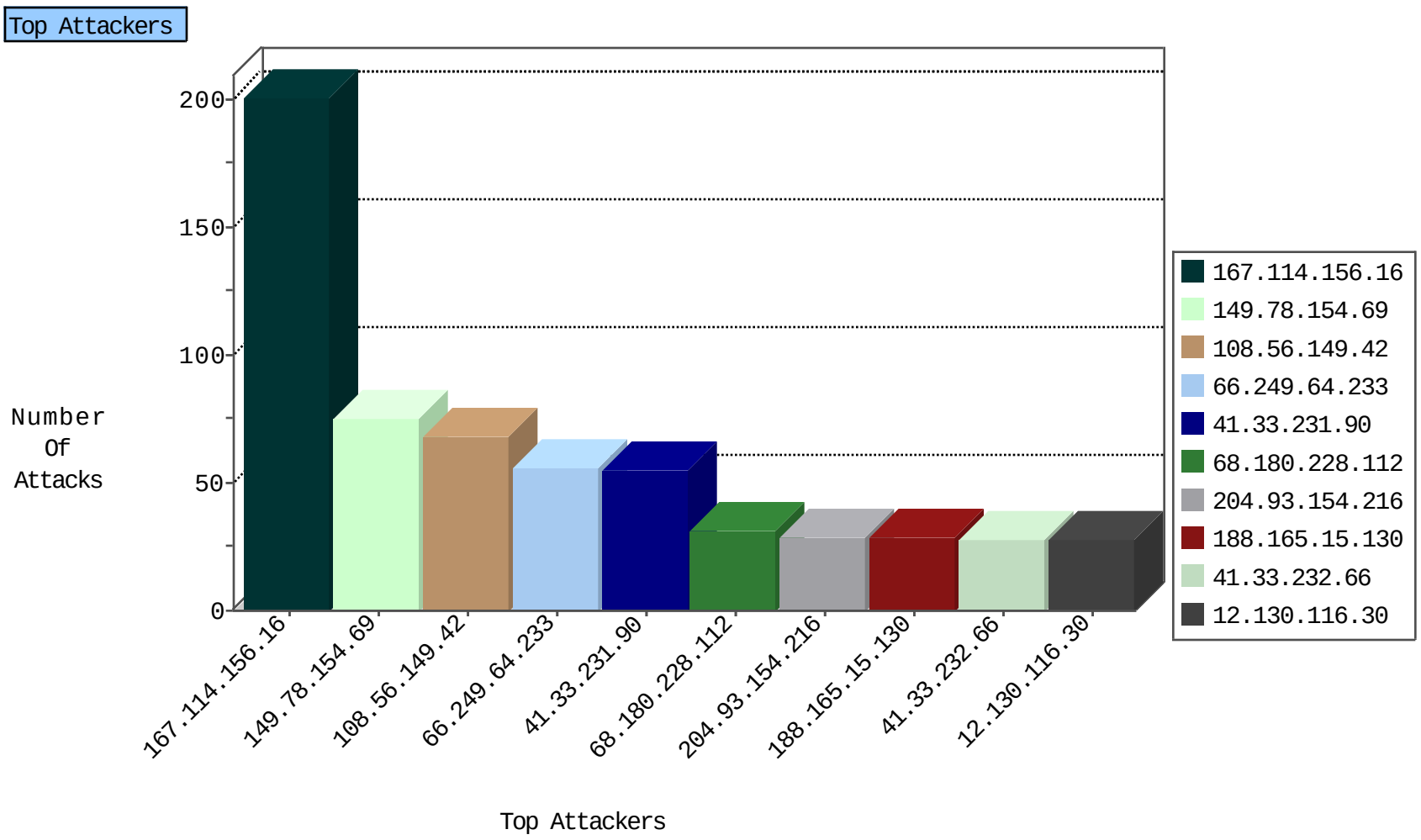
11-13-2015-03:04:02 to 11-13-2015-04:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-13-2015-03:04:02 to 11-13-2015-04:04:02

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	HTTP-POST-Segmented-DoS	dest-reset	8762
115.74.133.122	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5542
59.169.113.108	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3048
122.158.50.104	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2859
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1557
67.43.122.122	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	272
1.171.179.126	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	269
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	166
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	131
74.14.178.117	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
210.91.148.62	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	85
191.114.239.98	Chile	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70
223.88.146.100	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
220.181.108.187	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	52
71.46.180.77	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
126.22.81.34	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	15
184.170.63.119	Jamaica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	3
162.255.120.89	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
195.46.45.50	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
190.11.152.57	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
79.142.122.4	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
76.76.229.51	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
125.77.110.105	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
178.20.83.19	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
62.94.56.73	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
85.94.44.92	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
209.40.156.28	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
63.248.22.104	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
182.107.21.22	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
82.164.158.76	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
124.254.12.194	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
24.122.58.72	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
86.100.148.120	Lithuania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
169.157.227.107	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.150.231.30	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.51.50.77	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
210.22.116.66	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
70.112.69.76	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
107.14.71.28	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
59.190.49.190	Japan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
83.223.16.3	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
45.62.84.43		147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
81.191.88.2	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
131.252.130.90	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
67.193.98.120	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-13-2015-03:04:02 to 11-13-2015-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.132	France	147.237.77.176	matpash.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

11-13-2015-03:04:02 to 11-13-2015-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
157.232.94.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.42.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.6.108	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.117.93	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.140.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.36.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.90.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.59.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.175.110	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
83.229.69.36	147.237.76.196	Satellite Provider	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
199.89.17.117	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.113.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
142.54.163.74	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
109.94.212.125	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
211.151.127.21	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
170.113.200.87	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.24.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.226.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.179.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.196.39	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.76.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.241.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.214.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.55.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.29.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.133.74	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.33.85	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.198.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.125.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.191.15	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.50.197.147	147.237.0.15	Australia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
170.113.173.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.209.75	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.177.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
83.229.69.36	147.237.76.38	Satellite Provider	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.183.51.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.103.44	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.188.44	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.61.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.142.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.94.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.42.133.11	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.69.11	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.252.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.174.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.25.123	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.170.6	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.226.63	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.52.36	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-13-2015-03:04:02 to 11-13-2015-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.56.149.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	29
12.130.116.30	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
96.44.189.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
203.6.69.2	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
40.77.167.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.191.79	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.57.29		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.30	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
95.77.97.74	Romania	147.237.76.202	e.halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
101.184.57.246	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
125.202.25.184	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
162.243.73.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
70.50.80.26	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.48.37	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.27	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
207.46.13.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

11-13-2015-03:04:02 to 11-13-2015-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	4
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	4
85.250.15.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.127.231.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
141.212.122.80	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
69.171.228.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22925-he	Block	1
66.249.66.90	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation System.String[] in www.navy.idf.il/navy/general.aspx	Block	1
40.77.167.40	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/chinuch/faq/default.asp	None	1
157.55.39.200	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
69.171.230.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22925-he	Block	1
66.249.66.95	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspxense	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/5/size220x0/4435.jpg	Block	1
66.249.69.34	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
107.167.102.152	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18069	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/4435.jpg	Block	1
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
123.192.120.227	Taiwan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22925-he	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21050-h	Block	1
207.46.13.27	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.34.193	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

11-13-2015-03:04:02 to 11-13-2015-04:04:02