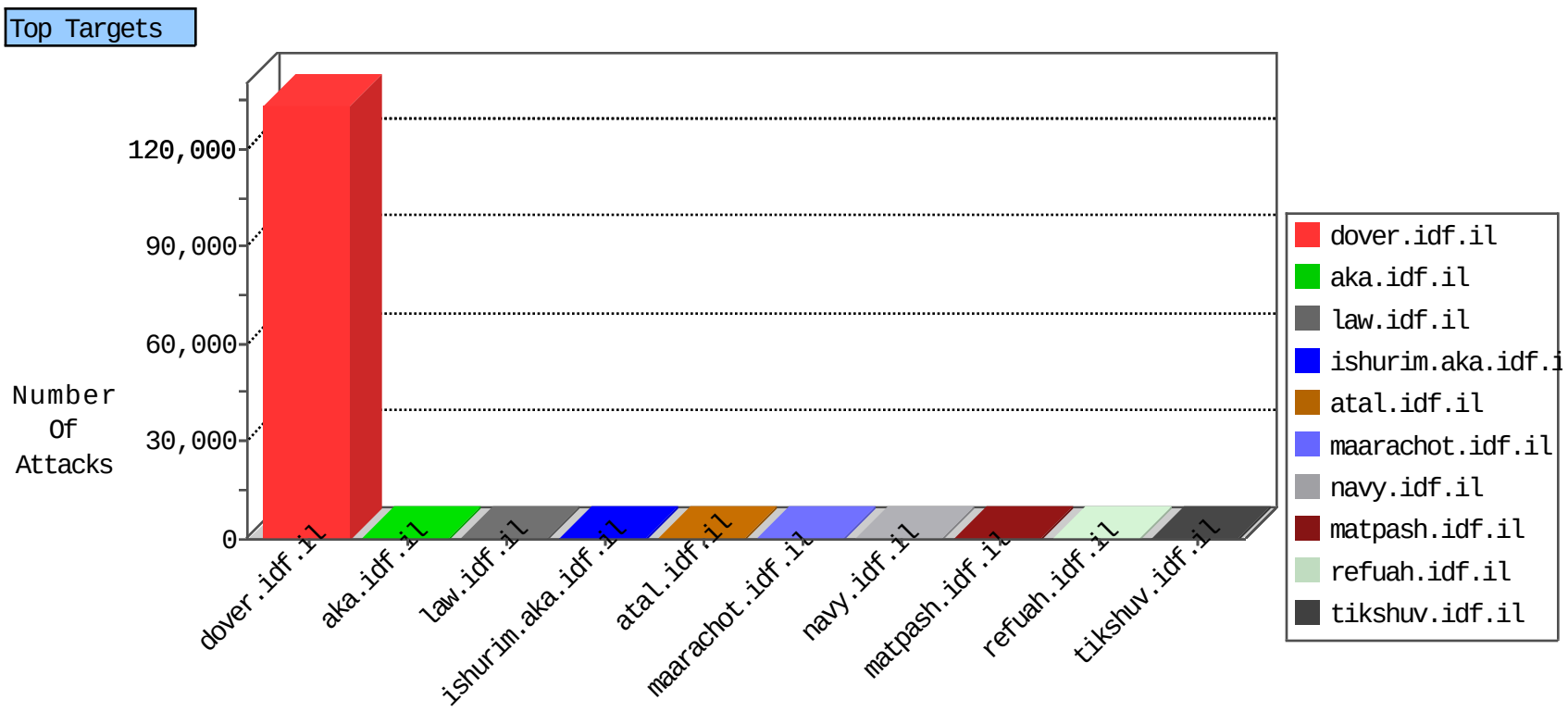
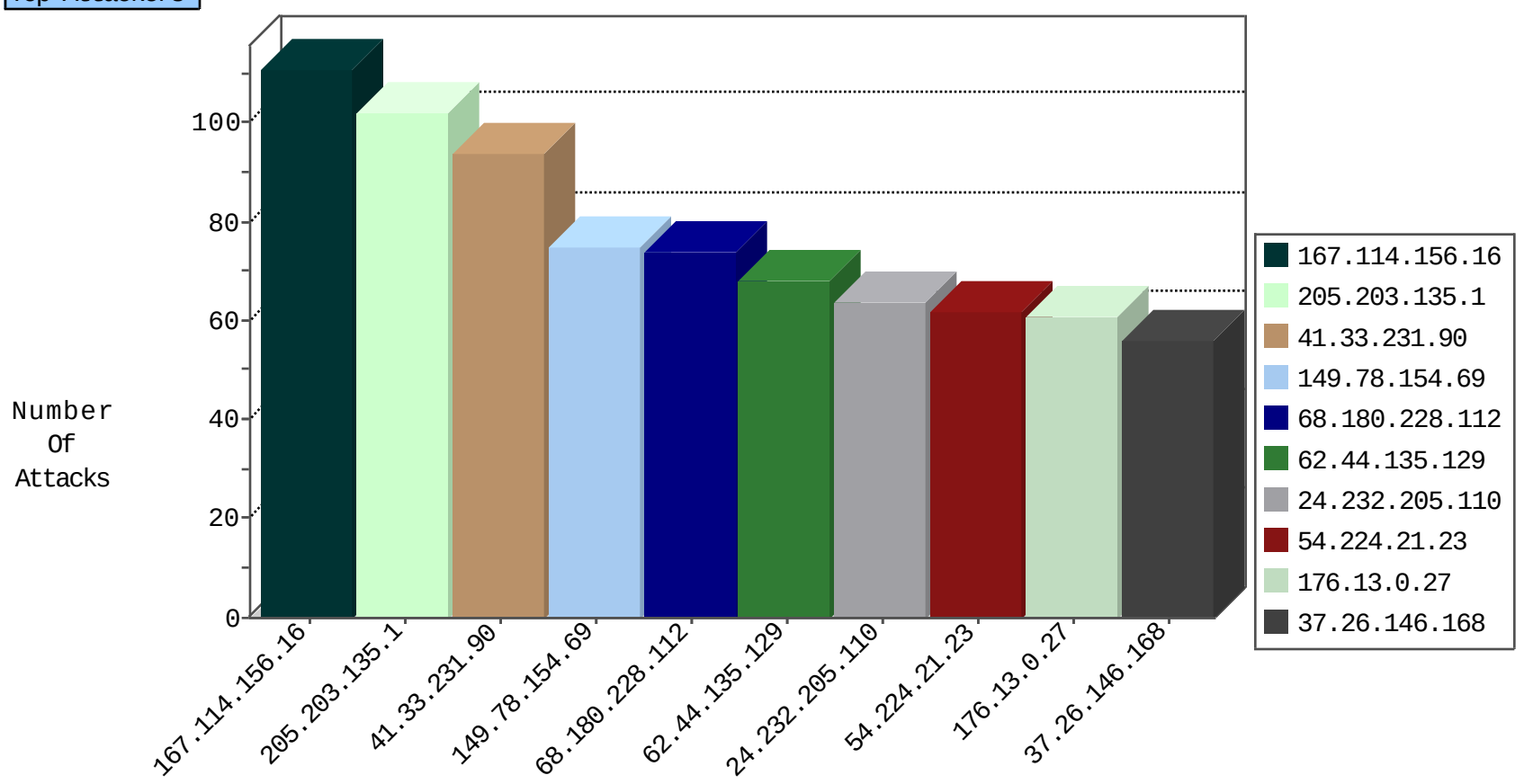
11-13-2015-02:04:09 to 11-13-2015-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-13-2015-02:04:09 to 11-13-2015-03:04:09

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	3468
126.80.225.122	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3140
97.78.86.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3104
106.246.119.50	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2860
126.88.93.38	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2845
111.93.146.66	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2752
160.198.15.95	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2730
151.139.89.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2694
101.108.72.81	Thailand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2692
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2012
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	527
183.40.232.21	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	452
37.238.180.51	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	405
189.80.157.68	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	276
119.197.21.36	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	245
126.218.186.81	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	244
183.123.232.7	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	238
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	207
126.88.194.119	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	177
171.213.0.127	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	177
174.100.201.7	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	160
85.30.152.71	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	143
184.229.75.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
79.159.20.103	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	110
83.42.138.73	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	110
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	109
174.98.68.67	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	102
179.119.31.79	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	94
124.230.149.36	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	88
81.100.246.44	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	77
221.8.129.7	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
14.95.219.81	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
183.103.54.67	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
106.84.118.1	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
126.12.1.110	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
113.169.141.103	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
121.128.145.114	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	18
119.225.32.9	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
123.133.193.88	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
220.181.108.181	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	8
97.107.214.83	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
219.116.68.6	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
72.38.208.122	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
63.248.78.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
131.191.52.5	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
74.196.113.75	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
81.2.102.58	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
84.111.241.91	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2

11-13-2015-02:04:09 to 11-13-2015-03:04:09

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	2
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.176	France	147.237.76.86	navy.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

11-13-2015-02:04:09 to 11-13-2015-03:04:09

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
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
170.106.167.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.182.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.189.16	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.203.240.39	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.238.7	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.245.71	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.204.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.174.11	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.181.70.28	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.64.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.44.128.57	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.214.9	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.107.73	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.241.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.108.20	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.144.188.46	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.114.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.149.63	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
148.178.6.49	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.208.91	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.103.49	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.184.89	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.169.100	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.155.22	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.153.4	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.40.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.89.105	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
170.67.223.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.105.154.110	147.237.77.216	Europe	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.140.91	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.161.83	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.227.47	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.198.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.94.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.51.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.134.10	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.52.255.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.234.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.74.121	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
170.67.120.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.204.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.100.17	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.106.52	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-13-2015-02:04:09 to 11-13-2015-03:04:09

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	102
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
62.44.135.129	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
24.232.205.110	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
176.13.0.27	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
37.26.146.168	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
79.178.196.20	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
93.169.160.225	Romania	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
17.142.152.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
173.243.45.162	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	28
37.46.39.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
17.142.152.68	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.102.8.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
17.142.152.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
62.128.35.245	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
52.29.4.122	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
100.127.192.229		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
104.235.196.7		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
104.197.104.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
85.130.253.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
85.250.181.249	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
188.40.112.210	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
37.142.64.9	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
52.28.85.70	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.102.8.238	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
37.46.39.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
128.242.249.13	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.13.19.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.177.108.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.253.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
219.74.38.12	Singapore	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
40.77.167.30	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11

11-13-2015-02:04:09 to 11-13-2015-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
23.96.208.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	2
197.52.158.88	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
66.249.79.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
109.64.60.18	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
38.99.190.240	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.123	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/klali/null	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId91 in www.aka.idf.il/patzar/klali/default.asp	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
40.77.167.30	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-22597-he	Block	1
157.55.39.250	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
217.31.48.13	Czech Republic	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/rom-0	Block	1
79.183.169.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
52.23.156.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
197.40.209.31	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
217.31.48.13	Czech Republic	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/rom-0	Block	1
104.235.106.142		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

11-13-2015-02:04:09 to 11-13-2015-03:04:09