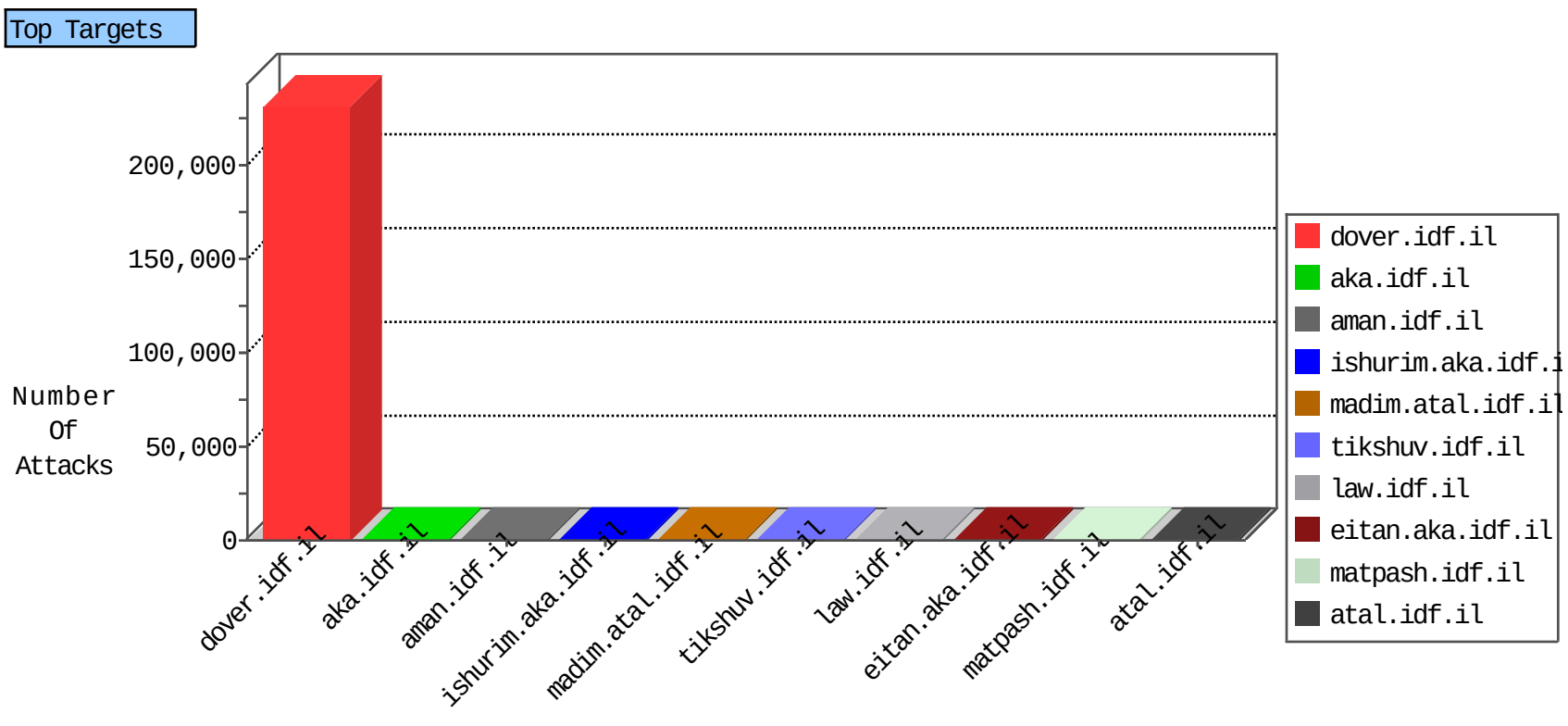
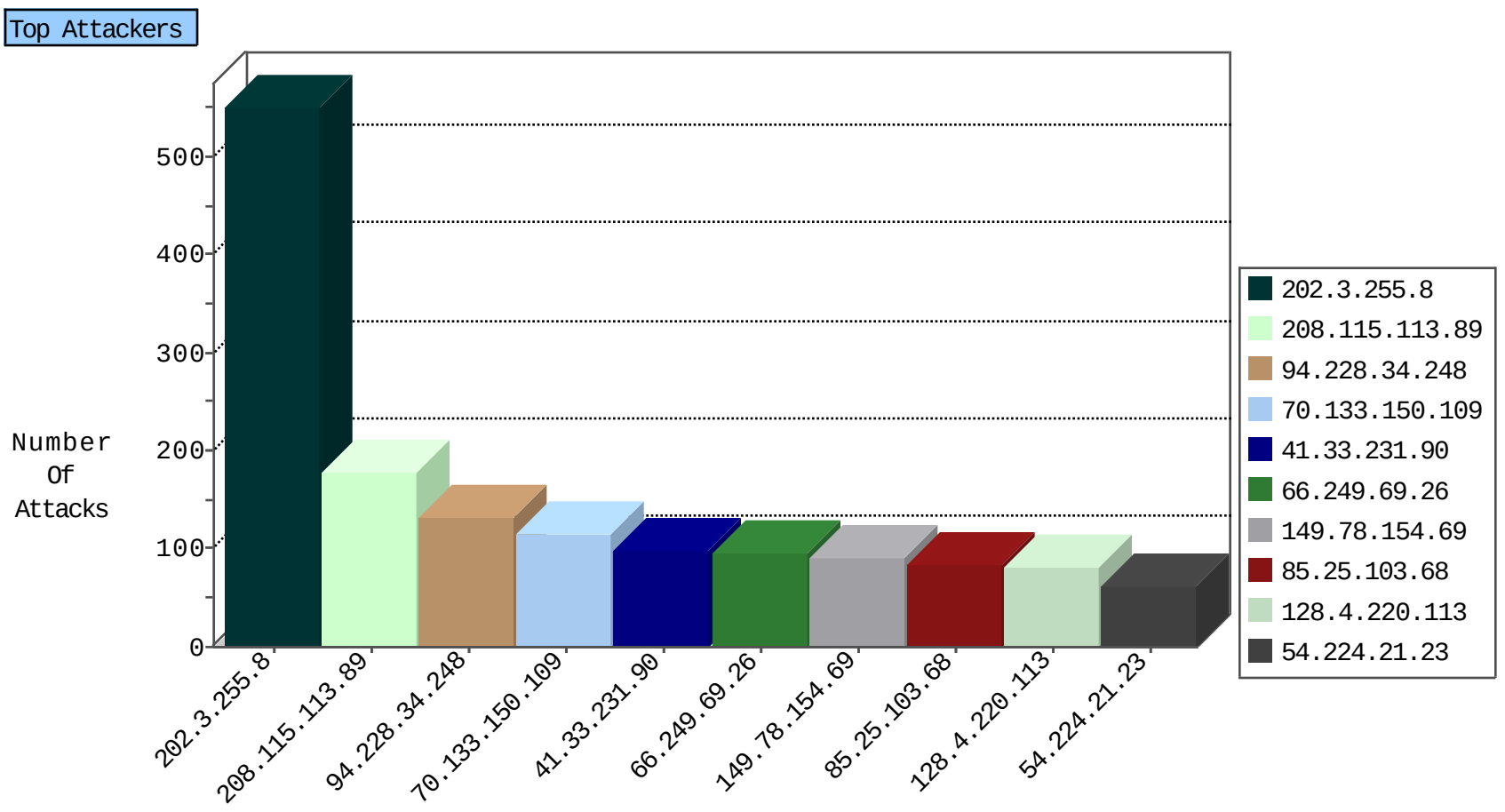
11-17-2015-04:04:04 to 11-17-2015-05:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-17-2015-04:04:04 to 11-17-2015-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.87.130.56	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5661
190.152.179.83	Ecuador	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3393
177.133.190.9	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3080
2.129.30.16	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3043
63.158.78.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3022
126.50.39.104	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2728
27.35.7.80	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2520
183.127.96.86	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	342
17.44.171.47	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	287
125.118.6.43	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	286
126.153.144.34	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	216
1.179.200.21	Thailand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	176
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	172
190.203.161.94	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
126.88.201.86	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	106
183.153.85.62	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	90
27.199.215.125	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	82
150.214.142.70	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70
42.61.112.97	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
220.94.52.91	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	49
155.223.144.59	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	45
1.32.100.100	Malaysia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36
126.78.58.65	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	29
58.214.183.109	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
126.145.108.47	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
91.147.236.19	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
63.248.230.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
70.63.47.107	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
24.235.162.72	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
113.255.221.98	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
84.202.46.29	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
67.22.86.105	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
216.172.84.64	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
47.60.147.94	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.125.13.31	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.53.136.84	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
119.234.24.7	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
69.170.74.11	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.59.76.56	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.178.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.29.112.46	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.92.61.16	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.187.59.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.168.78.108	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
152.3.218.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.114.184.58	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.160.108.70	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
202.154.240.18	Pakistan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.18.230.54	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-17-2015-04:04:04 to 11-17-2015-05:04:04

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	6
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-17-2015-04:04:04 to 11-17-2015-05:04:04

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	514
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.12.136.128	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
207.189.28.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.149.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.12.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.131.60.64	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.100.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.6.71.154	147.237.76.86	Poland	navy.idf.il	ET SCAN NMAP -sS window 1024	1
170.120.217.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.227.92.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.123.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.177.104	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
147.50.39.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.156.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.254.74	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.8.99	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.232.107	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.231.65.37	147.237.77.216	Colombia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.187.226.47	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.231.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.42.97	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.194.91	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.191.85	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.145.82	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.74.127	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.133.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.158.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.104.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.30.53	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.9.5	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.125.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.57.77.68	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.106.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
168.103.242.12	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.202.204.70	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.140.14	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.64.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.77.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.20.69.98	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
128.199.243.45	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.237.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.22.127.100	147.237.77.216	Netherlands	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.185.32.232	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
140.170.106.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.201.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
194.1.220.18	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.250.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-17-2015-04:04:04 to 11-17-2015-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	176
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
70.133.150.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
85.25.103.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
128.4.220.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
223.62.190.56	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
107.77.97.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.69.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
120.56.160.232	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
99.235.122.172	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.69.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
24.84.201.251	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.87.130.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
189.122.130.250	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
144.174.212.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.131.246.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
70.198.203.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.64.122.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.64.122.166	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.230.84.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.201.154.167	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
210.55.3.102	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.1.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.23.214	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
172.98.67.38		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
70.174.6.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.111.22.101	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
94.230.84.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7

11-17-2015-04:04:04 to 11-17-2015-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.151.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
168.235.194.242	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.194.242	Block	2
77.66.20.217	Denmark	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.73.220	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
176.12.151.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyujs/	Block	1
84.109.226.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.101	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
128.252.173.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.79.9	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-he	Block	1
94.159.203.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
141.212.122.80	United States	147.237.0.34	tikshuv.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	1
40.77.167.18	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/chinuch/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
168.235.194.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shjavascript	Block	1
80.178.24.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.50	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/writetous/default.asp	None	1
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1

11-17-2015-04:04:04 to 11-17-2015-05:04:04