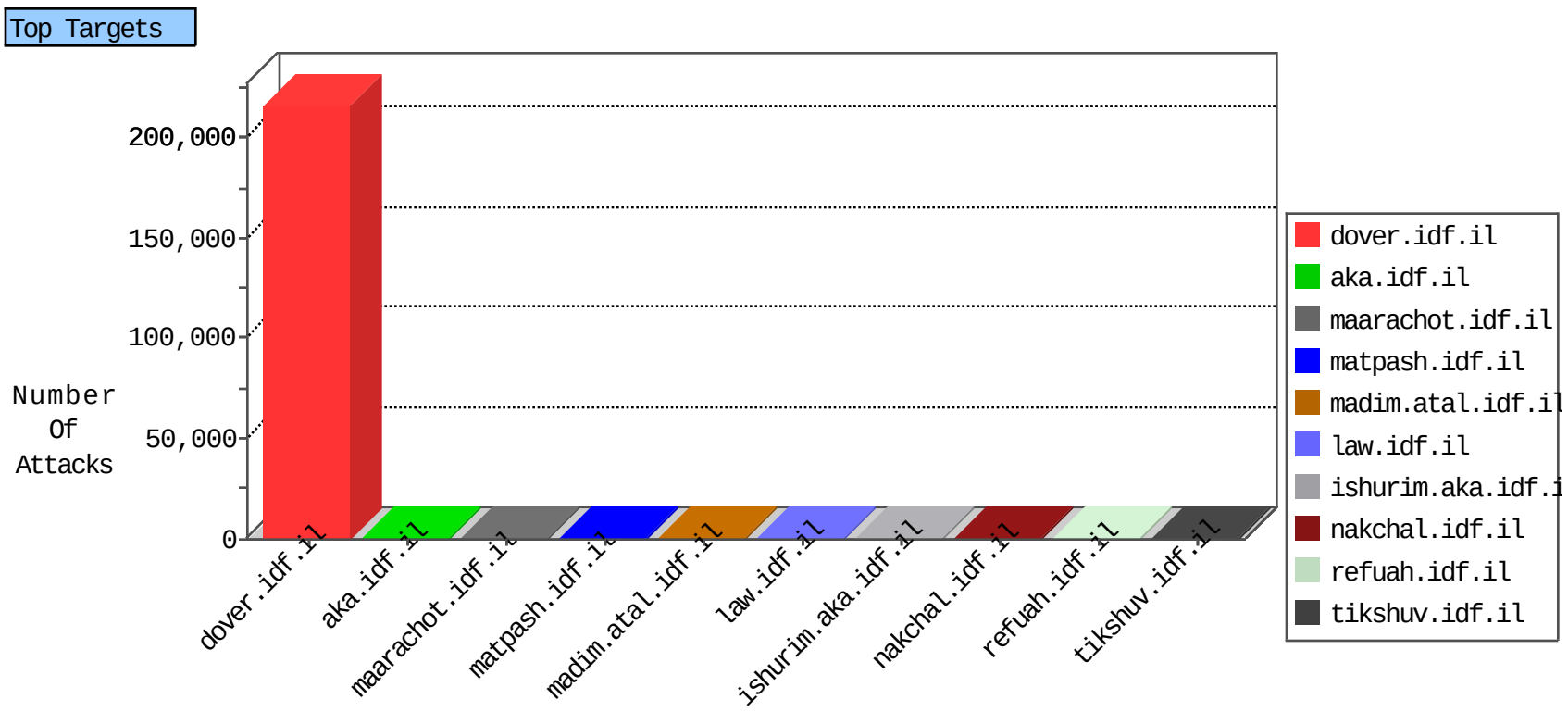
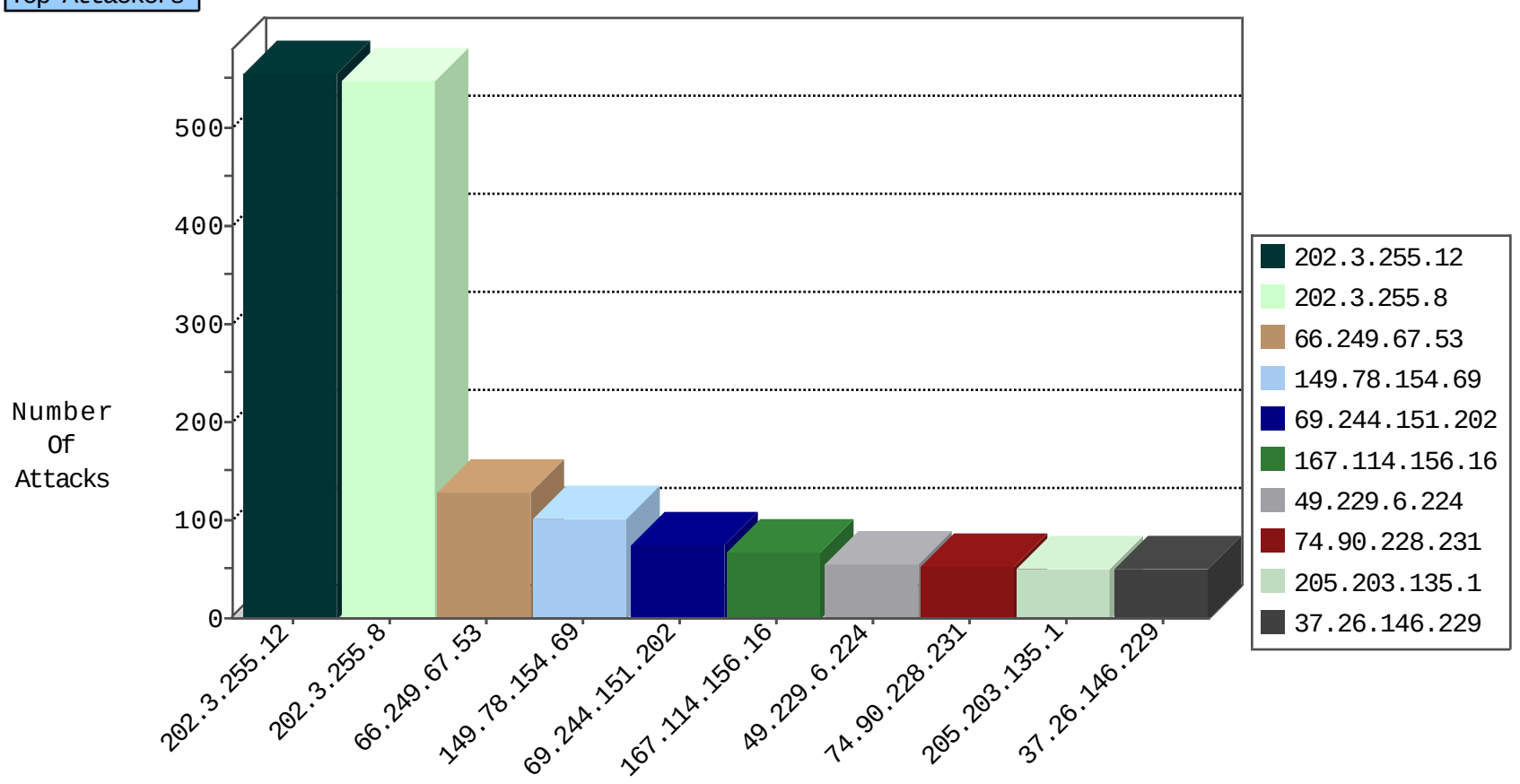
11-19-2015-05:04:03 to 11-19-2015-06:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-19-2015-05:04:03 to 11-19-2015-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.64	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3650
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2078
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	828
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	355
130.93.117.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
112.229.48.27	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
174.47.253.111	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
2.142.197.101	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.65.27.61	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
72.42.103.84	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
99.247.45.34	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
115.230.124.164	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
69.8.138.42	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
129.157.254.40	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
37.130.32.62	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.11.53.84	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.5.192.67	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.48.28	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.116.21	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.100.137.92	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.182.73.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
108.178.192.28	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.108.117	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
96.30.228.55	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
13.52.39.55	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
80.27.170.79	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
189.3.21.68	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.230.177.104	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.249.174.72	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.137.154.74	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.238.255.114	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.0.82.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.116.85.113	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.15.33.4	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
135.0.25.17	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.23.162.10	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.52.84.105	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.209.59.77	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.202.79.88	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.159.130.6	Mexico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
67.20.243.111	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
116.90.237.75	Nepal	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.139.132.53	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
99.237.104.57	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.136.232.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.239.204.48	France	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
193.165.72.12	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.63.169.58	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-19-2015-05:04:03 to 11-19-2015-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-19-2015-05:04:03 to 11-19-2015-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	519
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	511
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.218.216.220	147.237.77.170	Palestinian Territory, Occupied	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
191.243.51.34	147.237.76.148	Brazil	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
199.34.149.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.193.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.85.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
170.106.98.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.176.250.45	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
134.209.209.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.133.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
191.243.51.34	147.237.72.217	Brazil	e.idf.il	ET SCAN Potential SSH Scan	1
198.20.22.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.8.25	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.37.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
103.243.107.56	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN Potential SSH Scan	1
150.126.0.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
191.243.51.34	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
134.127.224.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.152.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.184.242.89	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.107.111	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
103.243.107.56	147.237.76.86	Vietnam	navy.idf.il	ET SCAN Potential SSH Scan	1
191.243.51.34	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
148.248.111.105	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
186.22.58.88	147.237.77.216	Argentina	dover.idf.il	ET DROP Dshield Block Listed Source	1
134.127.190.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.29.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.28.138.100	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
103.243.107.56	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Potential SSH Scan	1
191.243.51.34	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
140.170.70.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.6.122	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.51.42.163	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
130.201.130.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.113.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
103.243.107.56	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
191.243.51.34	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
138.43.144.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.83.37	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.100.79	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.245.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
69.244.151.202	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
95.216.11.9	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-19-2015-05:04:03 to 11-19-2015-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
69.244.151.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
49.229.6.224	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
74.90.228.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
37.26.146.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
212.199.63.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
184.155.163.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
149.78.167.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.90.204		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
173.21.190.227	United States	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	19
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
70.215.2.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	15
157.55.39.20	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.181.111.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
194.90.39.41	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
203.133.169.101	Korea, Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.66.118.148	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.159.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.93.233	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
153.92.126.135	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.20	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
157.55.39.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.88.164.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
85.250.197.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
67.182.210.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.246.124.92	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.230	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.87.118.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.227	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

11-19-2015-05:04:03 to 11-19-2015-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.177.131.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.234.157.254	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
31.186.228.93	United Kingdom	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
220.244.77.143	Australia	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 220.244.77.143 (sigalgs DoS Attack)	None	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
107.150.55.52	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
31.186.228.96	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
128.232.110.28	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
131.162.130.180	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-19-2015-05:04:03 to 11-19-2015-06:04:03