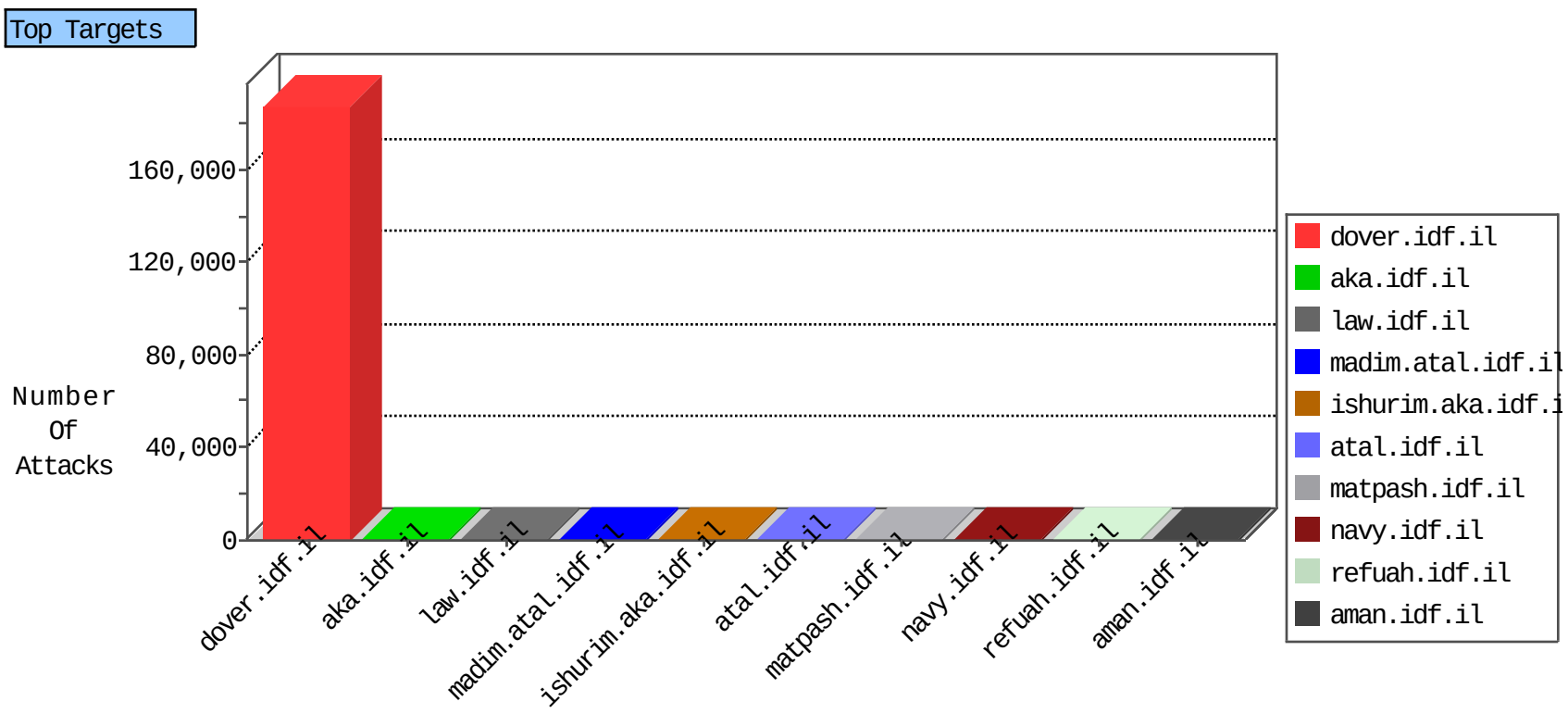
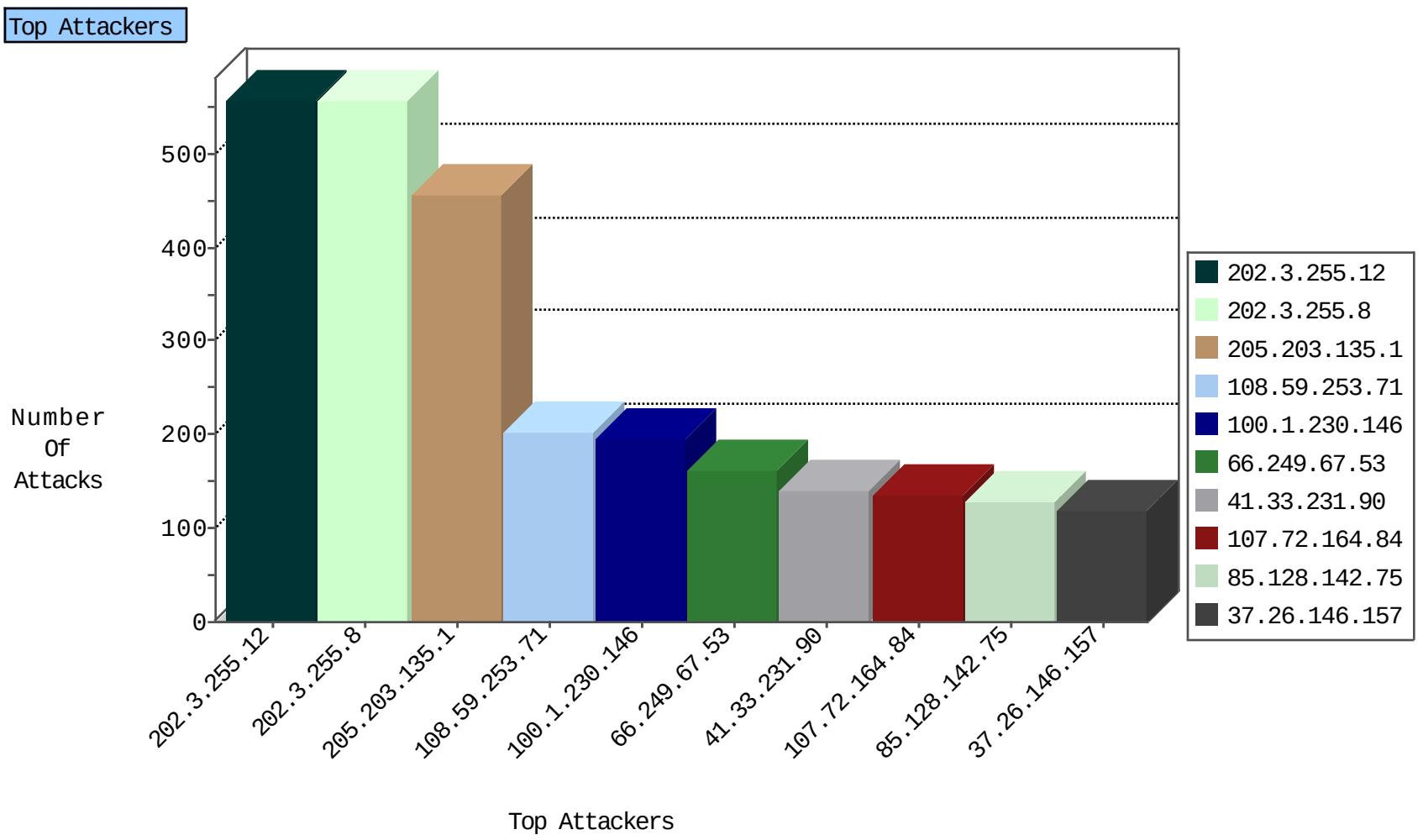
11-19-2015-03:04:07 to 11-19-2015-04:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-19-2015-03:04:07 to 11-19-2015-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13135
95.111.219.84	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5814
175.228.5.33	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3076
197.52.26.70	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2696
71.46.37.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2692
27.235.192.18	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2620
202.196.135.78	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	512
66.249.78.2	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	399
94.139.65.54	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	188
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	168
110.153.201.41	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	93
184.57.197.7	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	76
123.156.54.51	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	71
125.47.55.23	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	49
126.223.47.13	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
100.1.230.146	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
45.46.19.24		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
63.248.61.82	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
178.134.100.43	Georgia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.108.129.83	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.109.28.42	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
217.73.168.4	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.53.4.18	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.141.132.39	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
67.55.17.126	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
151.56.86.27	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.48.64.20	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.223.58	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.91.228.4	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.25.203.8	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
45.113.4.2		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
96.30.228.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
81.123.233.73	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.97.35.89	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
76.79.32.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.113.122.68	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.29.116.45	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.208.119	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.58.28.40	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.64.252.72	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.235.102.1	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.247.169.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.196.32	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.89.45	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.127.85.6	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.33.94.115	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
203.239.147.112	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.133.52	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.187.103	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-19-2015-03:04:07 to 11-19-2015-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.10.68.254	Netherlands	147.237.72.166	aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
5.10.68.254	Netherlands	147.237.77.233	atal.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	5
5.10.68.254	Netherlands	147.237.72.166	aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
5.10.68.254	Netherlands	147.237.77.233	atal.idf.i	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

11-19-2015-03:04:07 to 11-19-2015-04:04:07

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
202.3.255.12	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	4
110.20.7.193	147.237.0.33	Australia	idf.il	ET SCAN Potential SSH Scan	2
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.120.184.169	147.237.77.176	Taiwan	matpash.idf.il	GPL SCAN nmap TCP	2
157.231.105.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.227.196.29	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
95.216.62.92	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.68.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.29.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.200.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.174.93.68	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
148.248.217.104	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.10.68.254	147.237.72.166	Netherlands	aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
122.202.99.102	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.174.93.68	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
143.135.117.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.44.131.15	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.216.1	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.35.52.180	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
84.22.112.76	147.237.77.216	Netherlands	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.125.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.20.7.193	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
170.106.87.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.35.52.180	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
138.43.192.86	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.130.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.20.7.193	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
167.97.69.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.35.52.180	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
134.209.126.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
216.212.208.31	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.28.118.58	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.35.52.180	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
134.172.93.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.22.224.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.125.66.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.56.90.1	147.237.0.35	Romania	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.77.76.27	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
204.236.9.73	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.127.60.110	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.241.35	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.227.196.29	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
95.216.153.72	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-19-2015-03:04:07 to 11-19-2015-04:04:07

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	458
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	202
100.1.230.146	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	194
107.72.164.84	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	136
85.128.142.75	Poland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	128
66.249.67.53	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
37.26.146.157	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	118
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	109
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
107.77.68.58	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	76
24.232.205.110	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
37.26.146.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
27.67.41.249	Vietnam	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
46.163.68.109	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
84.228.59.66	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
208.80.155.255	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
37.26.148.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
99.238.49.154	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
66.249.67.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
66.249.67.59	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
69.119.203.80	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
157.55.39.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
209.6.148.106	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
207.46.13.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
207.46.13.160	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.116.122.228	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
183.79.219.188	Japan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	27
66.249.67.53	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
207.46.13.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
17.142.156.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
76.89.152.140	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
198.251.53.48	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
204.93.154.216	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
109.66.161.13	Israel	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.15.218	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
27.67.41.249	Vietnam	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	14

11-19-2015-03:04:07 to 11-19-2015-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.198.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.21.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
70.193.122.101	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20038-he/dover.aspx<span style='color:red	Block	1
141.212.122.96	United States	147.237.76.86	navy.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.19	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.19	Block	1
109.65.178.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
144.76.100.180	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 144.76.100.180	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2689.jpg	Block	1
144.76.100.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
184.105.139.67	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
131.162.130.180	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2418.jpg	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.160	Block	1
141.212.122.96	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
157.55.39.18	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

11-19-2015-03:04:07 to 11-19-2015-04:04:07