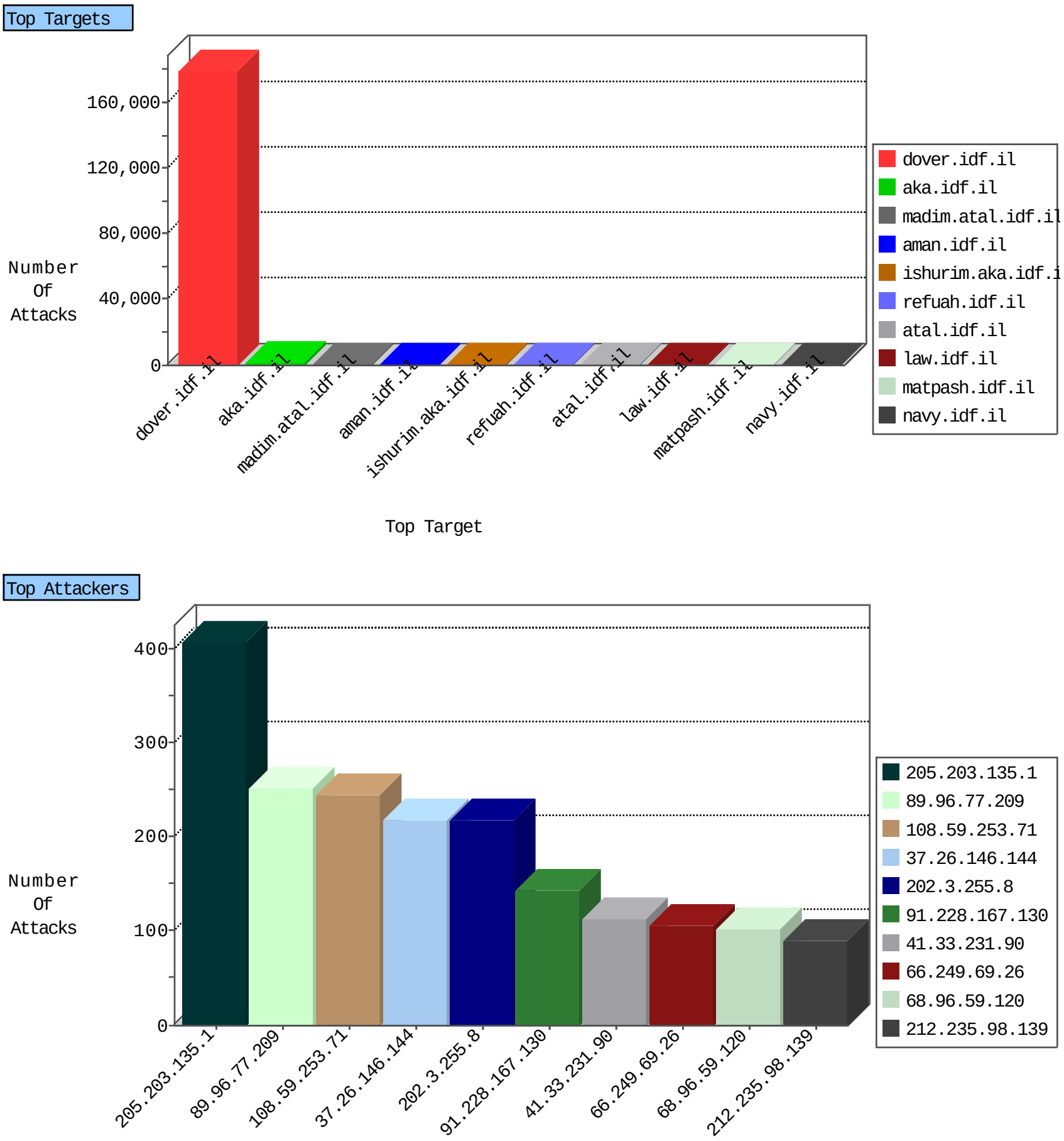
11-17-2015-15:04:08 to 11-17-2015-16:04:08

IDF Under Attack
Daily Report



11-17-2015-15:04:08 to 11-17-2015-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.159.44.244	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6275
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174
2.54.46.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	52
82.145.209.17	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	37
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	12
2.54.157.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
80.246.136.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.179.181.100	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.120.28.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.64.19.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
149.88.2.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
85.19.222.78	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
79.178.152.96	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
116.201.53.86	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
79.178.152.96	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
92.27.175.56	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
5.29.139.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
64.89.188.53	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.74.14.8	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.236.235.120	Austria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.219.201.71	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.175.34.62	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
113.12.71.38	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.242.36.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.229.209.23	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.197.136.12	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.108.112.8	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.88.139.43	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.33.88.126	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.170.222.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.106.94.11		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
63.248.63.54	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
144.80.80.113	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.215.0.28	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
219.116.70.20	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
105.235.105.96	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
12.205.247.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.198.92	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.178.152.96	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
201.220.158.60	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.252.246.67	Colombia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.253.110.74	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
70.79.233.42	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.186.89.89	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.66.41.67	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.49.8.98	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.107.82	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
113.73.149.89	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.8.233.102	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-17-2015-15:04:08 to 11-17-2015-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	18
188.165.15.130	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	11
188.165.15.201	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.139	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.139	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-17-2015-15:04:08 to 11-17-2015-16:04:08

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	186
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
157.232.57.52	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.117.121.60	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.247.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
143.135.58.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
132.74.58.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.110.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.106.227.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.216.67.34	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.20.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
170.106.106.22	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.183.191.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.28.242.63	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.211.222.42	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
158.69.208.175	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
29.18.174.82	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
157.231.99.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.227.81.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.141.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
140.170.127.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.200.74.117	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.250.22	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.11.76.121	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.216.212.12	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.176.118	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.166.137.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
170.120.250.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.178.144.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
170.67.49.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
167.28.102.104	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.174.171.104	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-17-2015-15:04:08 to 11-17-2015-16:04:08

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.il	drop	First packet isn't SYN	drop	408
89.96.77.209	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	253
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	246
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
68.96.59.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	88
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	86
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
52.21.137.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.26.148.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
5.29.35.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
79.183.28.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
52.3.19.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.201.170.219	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.0.55	Ireland	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
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.69.152		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
86.176.229.80	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.21.162.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.66.200.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
173.192.79.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
204.51.219.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	26
52.21.255.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.67.197.8	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.38.92		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
74.6.254.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.146.39.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
184.173.106.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
112.203.237.43	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.144	Block	125
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
37.26.149.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
85.64.16.140	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	12
85.64.16.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	12
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.179.23.113	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.179.23.113	Block	9
37.26.147.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.180.195.235	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
79.176.8.220	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	4
79.180.195.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	4
79.177.20.176	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.177.20.176	Block	4
208.115.111.72	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
79.176.8.220	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
207.241.226.42	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	3
212.235.55.246	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.55.246	Block	3
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.210.246.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.241.226.42	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	3
192.114.177.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
2.54.154.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.41.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.7.14.25	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	2
87.68.36.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.188.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.19.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.29.102.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.179.14.123	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
132.70.66.11	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1148-he/atal.aspx	Block	2
79.183.117.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
93.172.51.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.160.99	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.183.180.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.186.42	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
109.65.5.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.53.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	1
176.12.137.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.97.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
85.64.20.149	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.120	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
79.178.152.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.135	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/forms.aspx	Block	1
109.66.29.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	1
31.154.190.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.23.113	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
185.32.179.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1