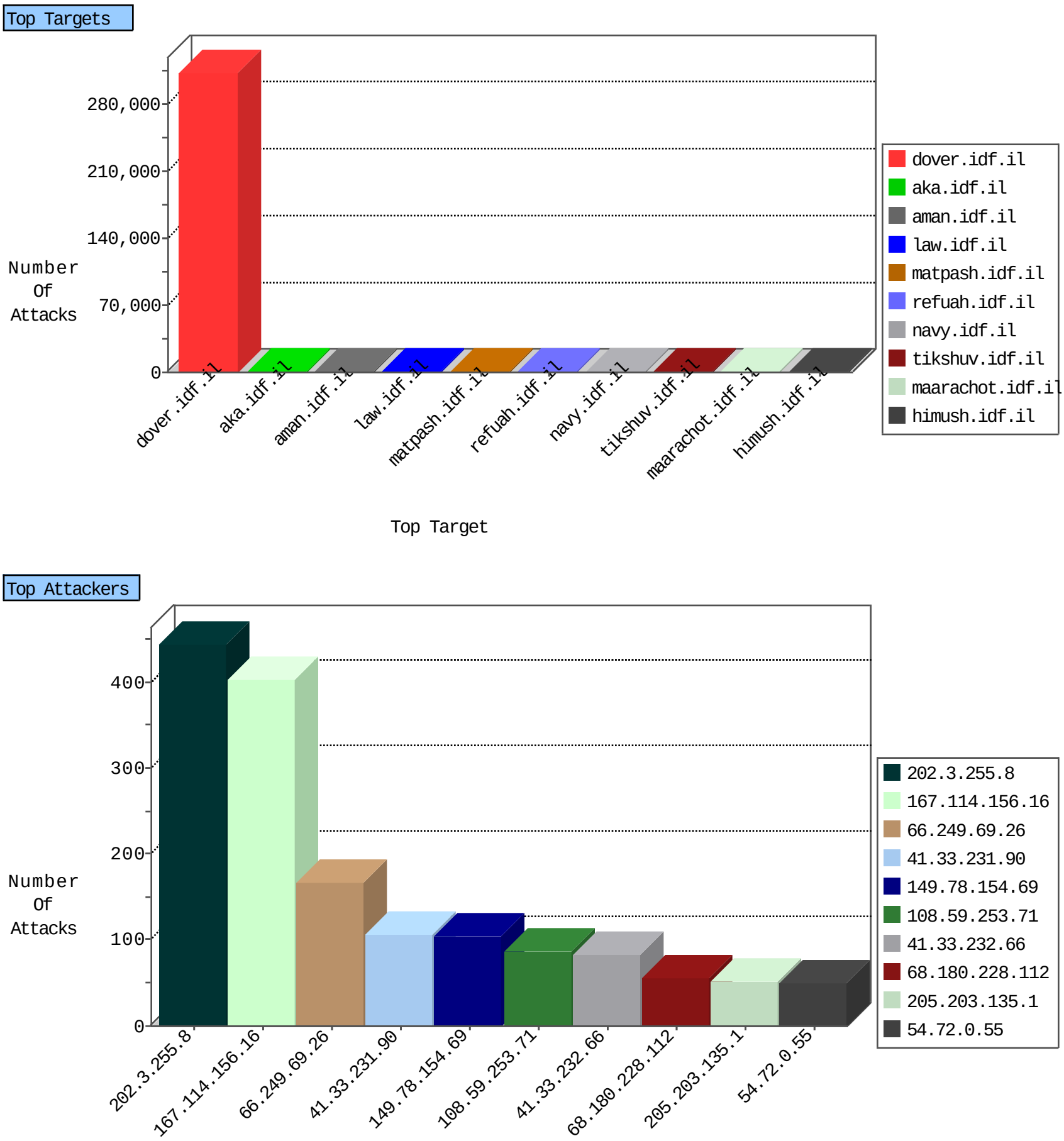
11-17-2015-06:04:01 to 11-17-2015-07:04:01

IDF Under Attack Daily Report



11-17-2015-06:04:01 to 11-17-2015-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.9.54	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	7161
66.249.64.92	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4207
66.249.73.228	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3385
189.104.16.10	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3153
60.13.181.111	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2752
73.52.172.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2732
117.239.217.63	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2647
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	777
66.249.64.102	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	500
49.249.232.30	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	297
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	256
85.28.224.49	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	226
80.22.3.94	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	191
122.11.137.18	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	190
172.72.41.15		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	184
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	178
71.93.80.39	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	174
117.197.64.2	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	152
17.141.62.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	152
187.160.6.13	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	135
46.70.137.50	Armenia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	125
114.120.198.92	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	119
24.24.56.92	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79
160.15.19.59	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
138.101.248.8	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
164.138.125.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	52
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	39
156.145.115.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34
39.164.255.0	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33
121.216.221.91	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
27.77.228.105	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
130.212.96.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
2.193.219.19	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
196.47.189.21	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
79.99.18.10	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
66.185.202.93	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.129.57.72	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
66.211.233.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
66.182.81.42	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
94.72.122.118	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
70.123.16.68	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
109.88.189.1	Belgium	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
178.219.121.5	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.238.94.116	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
133.46.212.91	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
216.58.101.122	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.13.16.66	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
83.92.115.7	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
126.219.102.77	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-17-2015-06:04:01 to 11-17-2015-07:04:01

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	8
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	6
151.80.31.131	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	2
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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
185.106.94.2		147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1

11-17-2015-06:04:01 to 11-17-2015-07:04:01

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	411
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	3
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
170.113.93.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.20.169.71	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.51.46.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.30.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.137.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.132.107	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.83.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.152.124	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.235.254.181	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
207.22.223.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.139.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.15.66	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.67.220.16	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.213.119	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.192.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.148.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.235.2.9	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.189.71.43	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.83.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.205.71	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
98.102.200.172	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
130.201.144.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.168.123	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.58	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.219.144.43	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.236.20.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.80.67	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.148.216.99	147.237.77.216	United Kingdom	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.218.83	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.137.54	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.77.88	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.179.61.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.47.197.110	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.109.108	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.150.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.102.186.35	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
162.125.112.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.15.33	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.93.154.216	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
148.178.112.118	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.50.99	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.3.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.18.10	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.121.27	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.194.88	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
200.105.35.40	147.237.77.216	Argentina	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-17-2015-06:04:01 to 11-17-2015-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	355
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
128.252.25.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
113.197.14.2	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.69.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.69.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
203.135.187.11	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
203.135.187.11	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.3.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.102.9.101	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
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.65.121.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
168.63.137.102	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
176.13.6.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.42.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.102.9.54	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.20.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.12.138.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.86.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

11-17-2015-06:04:01 to 11-17-2015-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.64.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.106.94.2		147.237.72.166	aka.idf.il	Multiple URL worm attacks from 185.106.94.2	Block	2
109.201.154.240	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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-ar/cogat.aspx	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.106.94.2		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/cgi-bin/php	Block	1
87.68.45.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
222.246.179.203	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
141.212.122.80	United States	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
69.58.178.58	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
203.135.187.11	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/+navmenu.qc+	Block	1
104.173.18.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
141.212.122.80	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
46.116.107.200	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8754-he/refuah.aspx	Block	1
185.106.94.2		147.237.72.166	aka.idf.il	Access to: /cgi-bin/php5	Block	1
79.178.141.77	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.178.141.77 (sigalgs DoS Attack)	None	1
46.116.107.200	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.116.107.200	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.141.77	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1

11-17-2015-06:04:01 to 11-17-2015-07:04:01